# IDENTITY THEFT: IS THERE ANOTHER YOU?

## JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON TELECOMMUNICATIONS, TRADE, AND CONSUMER PROTECTION

AND THE

SUBCOMMITTEE ON FINANCE AND HAZARDOUS MATERIALS

OF THE

COMMITTEE ON COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTH CONGRESS

FIRST SESSION

APRIL 22, 1999

**Serial No. 106–16**

Printed for the use of the Committee on Commerce

U.S. GOVERNMENT PRINTING OFFICE
56–605CC WASHINGTON : 1999

## COMMITTEE ON COMMERCE

TOM BLILEY, Virginia, *Chairman*

W.J. "BILLY" TAUZIN, Louisiana
MICHAEL G. OXLEY, Ohio
MICHAEL BILIRAKIS, Florida
JOE BARTON, Texas
FRED UPTON, Michigan
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
*Vice Chairman*
JAMES C. GREENWOOD, Pennsylvania
CHRISTOPHER COX, California
NATHAN DEAL, Georgia
STEVE LARGENT, Oklahoma
RICHARD BURR, North Carolina
BRIAN P. BILBRAY, California
ED WHITFIELD, Kentucky
GREG GANSKE, Iowa
CHARLIE NORWOOD, Georgia
TOM A. COBURN, Oklahoma
RICK LAZIO, New York
BARBARA CUBIN, Wyoming
JAMES E. ROGAN, California
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
JOHN B. SHADEGG, Arizona
CHARLES W. "CHIP" PICKERING, Mississippi
VITO FOSSELLA, New York
ROY BLUNT, Missouri
ED BRYANT, Tennessee
ROBERT L. EHRLICH, Jr., Maryland

JOHN D. DINGELL, Michigan
HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
RALPH M. HALL, Texas
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
FRANK PALLONE, Jr., New Jersey
SHERROD BROWN, Ohio
BART GORDON, Tennessee
PETER DEUTSCH, Florida
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
RON KLINK, Pennsylvania
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
THOMAS C. SAWYER, Ohio
ALBERT R. WYNN, Maryland
GENE GREEN, Texas
KAREN MCCARTHY, Missouri
TED STRICKLAND, Ohio
DIANA DEGETTE, Colorado
THOMAS M. BARRETT, Wisconsin
BILL LUTHER, Minnesota
LOIS CAPPS, California

JAMES E. DERDERIAN, *Chief of Staff*
JAMES D. BARNETTE, *General Counsel*
REID P.F. STUNTZ, *Minority Staff Director and Chief Counsel*

---

## SUBCOMMITTEE ON TELECOMMUNICATIONS, TRADE, AND CONSUMER PROTECTION

W.J. "BILLY" TAUZIN, Louisiana, *Chairman*

MICHAEL G. OXLEY, Ohio,
*Vice Chairman*
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
CHRISTOPHER COX, California
NATHAN DEAL, Georgia
STEVE LARGENT, Oklahoma
BARBARA CUBIN, Wyoming
JAMES E. ROGAN, California
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
CHARLES W. "CHIP" PICKERING, Mississippi
VITO FOSSELLA, New York
ROY BLUNT, Missouri
ROBERT L. EHRLICH, Jr., Maryland
TOM BLILEY, Virginia,
(Ex Officio)

EDWARD J. MARKEY, Massachusetts
RICK BOUCHER, Virginia
BART GORDON, Tennessee
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
ELIOT L. ENGEL, New York
ALBERT R. WYNN, Maryland
BILL LUTHER, Minnesota
RON KLINK, Pennsylvania
THOMAS C. SAWYER, Ohio
GENE GREEN, Texas
KAREN MCCARTHY, Missouri
JOHN D. DINGELL, Michigan,
(Ex Officio)

SUBCOMMITTEE ON FINANCE AND HAZARDOUS MATERIALS

MICHAEL G. OXLEY, Ohio, *Chairman*

W.J. "BILLY" TAUZIN, Louisiana
*Vice Chairman*
PAUL E. GILLMOR, Ohio
JAMES C. GREENWOOD, Pennsylvania
CHRISTOPHER COX, California
STEVE LARGENT, Oklahoma
BRIAN P. BILBRAY, California
GREG GANSKE, Iowa
RICK LAZIO, New York
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
JOHN B. SHADEGG, Arizona
VITO FOSSELLA, New York
ROY BLUNT, Missouri
ROBERT L. EHRLICH, Jr., Maryland
TOM BLILEY, Virginia,
(Ex Officio)

EDOLPHUS TOWNS, New York
PETER DEUTSCH, Florida
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
DIANA DEGETTE, Colorado
THOMAS M. BARRETT, Wisconsin
BILL LUTHER, Minnesota
LOIS CAPPS, California
EDWARD J. MARKEY, Massachusetts
RALPH M. HALL, Texas
FRANK PALLONE, Jr., New Jersey
BOBBY L. RUSH, Illinois
JOHN D. DINGELL, Michigan,
(Ex Officio)

# CONTENTS


Page

Testimony of:
- Albright, Charles A., Chief Credit Officer, Household International, Inc ... 23
- Anderson, Robert, Mineral, Virginia ..... 11
- Bernstein, Joan Z., Director, Bureau of Consumer Protection, Federal Trade Commission ..... 16
- Connelly, D. Barry, President, Associated Credit Bureaus, Inc ..... 27

Material submitted for the record by:

# IDENTITY THEFT: IS THERE ANOTHER YOU?

**THURSDAY, APRIL 22, 1999**

HOUSE OF REPRESENTATIVES,
COMMITTEE ON COMMERCE,
SUBCOMMITTEE ON TELECOMMUNICATIONS,
TRADE, AND CONSUMER PROTECTION, JOINT WITH
SUBCOMMITTEE ON FINANCE AND HAZARDOUS MATERIALS,
*Washington, D.C.*

The subcommittee met, pursuant to notice, at 10 a.m., in room 2123, Rayburn House Office Building, Hon. W.J. "Billy" Tauzin (chairman) presiding.

Members present from the Subcommittee on Telecommuncations, Trade and Consumer Protection: Representatives Tauzin, Oxley, Deal, Shimkus, Wilson, Fossella, Blunt, Bliley (ex officio), Markey, Luther and Sawyer.

Members present from Subcommittee on Finance and Hazardous Materials: Representatives Oxley, Tauzin, Ganske, Shimkus, Wilson, Shadegg, Fossella, Blunt, Bliley (ex officio), DeGette, Barrett, Luther and Markey.

Staff present: Linda Rich, majority counsel; Robert Gordon, majority counsel; Brian McCullough, professional staff member; Robert Simison, legislative clerk; Consuela Washington, minority counsel; and Bruce Gwinn, minority professional staff.

Mr. TAUZIN. The committee will please come to order.

Good morning. Today's hearing is on identity theft—how it occurs, whether the anti-fraud laws are being enforced properly, and what can we do to help innocent people clean up their credit records after they have been victimized by an identity theft criminal.

While we are sitting here today, each one of us may unknowingly be the victim of identity theft. Some person might be searching through our mailbox or hacking our consumer accounts over the Internet to obtain the names, addresses and Social Security numbers of ourselves or our families. The thief then uses that information to open up lines of credit and go on a spending spree perhaps, all under someone else's identity.

As victims, we might not find out about this identity theft until several months later when the collection agencies start calling and we get turned down for a mortgage or credit loan, and then the real consumer nightmare begins.

Repairing your credit record, like trying to get rid of IRS liens, after you have been victimized by identity theft can take years of constant phone calls and letters trying to establish your innocence

to creditors you have never heard of. How can we end this kind of devastation and protect innocent victims?

Today we are fortunate to have with us the Director of Consumer Protection of the Federal Trade Commission, Jodie Bernstein, who will talk to us about the prosecution of identity theft and what sort of safeguards victims have under current law. Last year, Congress enacted the Identity Theft and Assumption Act to make identity theft a Federal crime and to empower the FTC to help victims repair their credit records. But we have over 500,000 credit fraud victims every year, and only a small fraction are ever actually prosecuted. I will be interested in hearing how the Federal Trade Commission is implementing this new law and how far their efforts will take us in helping innocent victims.

One such victim of identity theft is Bob Anderson, who is with us today from Mineral, Virginia. He was unable to refinance his mortgage because an identity thief stole his Social Security number and used that information to charge up bills on his account. Five years later, Mr. Anderson, believe it or not, is still trying to get his name cleared and his identity back.

Mr. Anderson's experience raises the critical question of how we should allocate the responsibility for fixing the damaged credit card and the credit record of an innocent victim. For example, what responsibility should be shared by the companies which granted the improper credit, especially to notify the appropriate organizations of potential fraud and suspend any payment claims? What responsibility should credit bureaus have to verify identity theft and to help clean up a credit report, notify all of the creditors? What sort of timeframe can we create to ensure that innocent victims like Mr. Anderson don't have to suffer through a nightmare that lasts for 5 long years and it is still not over?

Mr. Connelly and Mr. Albright will enlighten us as to the special problems facing credit bureaus and finance companies, and hopefully they can offer us some guidance on how we can better help victims like Mr. Anderson in the future, a future that will be punctuated with more and more electronic commerce and more and more opportunities for people to steal someone's identity and improperly take their credit and their good name with them.

We need better enforcement and prosecution of our anti-fraud laws. We need a system that helps, not ignores, the victims of identity theft; and today we will begin how, with the absolute minimum of Federal intrusion, we can still make a system work to protect the victims of identity theft, help them clear up their records in a timely fashion.

Additionally, I would like to thank my good friend, Mr. Oxley, for co-chairing this important event and look forward to working with him on this important issue. This is an issue that crosses the jurisdiction of our two committees in which we both work together as chairman and co-chairman, and so I am pleased to have Mr. Oxley join me in this hearing and will yield to him and then welcome the chairman of our full committee in just a second.

Mr. Oxley.

Mr. OXLEY. Thank you. As the gentleman from Louisiana indicated, both subcommittees are looking into this; and I have to say

that the title of our hearing probably says it best: Identity Theft: Is There Another You?

I was looking at the information from the Better Business Bureau that was just released, and it is headlined, San Diego, a man who knows baseball star Tony Gwynn's bank account, Social Security and driver's license numbers and his mother's maiden name recently cashed a $950 check at Anaheim. Also, someone has used Gwynn's name to test drive a Ford Escort and has yet to return the car. It says, anybody, even Tony Gwynn, can become a victim of identity fraud. And this person that tried to steal Tony Gwynn's identity couldn't steal his batting stroke; but it does show, I think, the ever-increasing dangers behind the identity theft problem. It is a phenomenon that has developed in concert with the growth of pin numbers and credit cards and other conveniences that improve the way that people and businesses engage in everyday transactions.

Identity theft occurs primarily in the area of financial services because, when someone is stealing another's identity, it is generally to get at their bank account or investment account or credit card account.

Identity theft, thanks to our colleague on the committee, Mr. Shadegg, is now a crime. There have been countless stories of people whose lives were ruined as a result of a thief who destroyed their credit, making it impossible for the victim to get a mortgage for a home, open a bank account or even get or keep a job. Indeed, we have one such victim testifying today who will help us understand just how damaging identity theft can be.

The Identity Theft and Assumption Deterrence Act of 1998, which Mr. Shadegg introduced and was signed into law last Congress, is an important step toward putting a stop to this crime. Law enforcement now has a tool to go after identity thieves for stealing a person's identity for the purpose of engaging in fraudulent activities.

The act also directed the FTC to take steps to help consumers who are victims of identity theft, including helping them repair their fraudulently damaged credit records. It is simply unconscionable that victims of identity theft have to suffer not only the personal damage done to them by the thieves but also from the frustration of being unable to promptly correct credit records that reflect bad debts run up, not by them, but by a criminal.

Under the Fair Credit Reporting Act, credit reporting agencies are responsible for correcting inaccurate information in credit reports. Based on the testimony of Mr. Anderson, as well as numerous stories of identity theft victims who have found it difficult, if not impossible, to correct credit reports that have been damaged by an identity thief, it seems that something is not working the way that it should.

A victim of identity theft should not have to battle with credit card issuers or credit reporting agencies to clear up his or her record if there is adequate evidence that a fraud has been committed. Unfortunately, that has been the experience of our first witness today, Mr. Anderson, who spent nearly 5 years working to clear up the damage done to his credit by an identity thief.

Thank you for coming today, Mr. Anderson, and sharing your experiences with the subcommittees; and I hope we can develop a

way to remedy this problem so others don't continue to face the same problems that you did.

The Federal Trade Commission, which has responsibility for administering the Fair Credit Reporting Act as well as the Identity Theft and Assumption Deterrence Act, among other statutes relating to this problem, has undertaken several initiatives to help educate and protect consumers from identity theft. I look forward to learning from the Federal Trade Commission what they are doing to ensure that victims are able to clear up their credit records once a fraud has been discovered.

Mr. Connelly, the President of the Associated Credit Bureaus, will indicate what steps credit bureaus are taking to facilitate and expedite the clearing up of fraudulently damaged credit records.

Today we will learn how a finance company that is a credit card issuer tackles the thorny issue of identity theft. After all, the card issuer generally absorbs the lion's share of the bad charges run up by an identity thief. The issuer has a strong incentive to put measures into place to prevent the fraud from happening in the first place.

I thank all of our witnesses for joining us today and look forward to both subcommittees learning more about this ever-growing problem, and I yield back.

Mr. TAUZIN. I thank my friend, the chairman of the Finance Committee, for his opening statement.

Bill, with your forbearance, I will now recognize the chairman of the full committee.

When the chairman of the full committee shows up at a subcommittee hearing, it means that we are doing something pretty important, so I want to recognize him and thank him for coming.

By the way, Mr. Chairman, this hearing reminds me of the old story of the lady in Washington who woke up in the middle of the night and said to her husband, wake up, honey; I think there is a thief in the house. He said, oh, go back to sleep; there are at least a dozen of them in the Senate.

The Chairman of the full Committee on Commerce, Tom Bliley.

Chairman BLILEY. Thank you, Mr. Chairman.

The Subcommittees on Telecommunications, Trade and Consumer Protection and on Finance and Hazardous Materials will be examining an issue of enormous significance to every American consumer and business. The issue is the growing problem of identity theft. This crime not only results in significant losses to businesses as a result of bills incurred by identity thieves who never intend to pay those debts, but also exacts terrible tolls on the victim's personal life before he or she even knows it is happening. We will hear today that victims of identity theft often do not discover this fraud until he or she can least afford it, when applying for credit or for a loan. That is a time when a victim of identity theft is informed of bad debts that do not belong to them.

The victims of identity theft suffer substantially. Not only is their credit hurt but all of the problems associated with a crime fall on their shoulders through no fault of their own. Long after the damage is done, the victim is burdened with continual problems of repairing his credit record, in fighting claims against him by the businesses the perpetrator has bilked. All because a thief was able

to acquire personal identification such as a Social Security number or credit card number and assume the victim's identity.

Fortunately, our colleague from Arizona, Mr. Shadegg, took it upon himself to move legislation to address this problem. While there were several statutes that prohibit fraud and relate to identity theft prior to the enactment of the Identity Theft and Assumption Act of 1998, there was no Federal law that criminalized the act of stealing another's identity. This lapse made it extremely difficult for victims of identity theft to have any recourse against the thieves who caused them such great personal expense.

The new law makes it a Federal crime to steal someone's identity and increases the penalties for the criminals. Additionally, the law requires the Federal Trade Commission to take actions to help the victims of these terrible crimes.

I welcome our witnesses today and look forward to hearing how the new act and other laws administered by the FTC are working—or not—to protect consumers and businesses from the damage done by identity thieves.

I would like to extend a special welcome to my fellow Virginian, Bob Anderson, who has suffered a great deal as a result of having been a victim of this crime.

I also thank our witnesses from the Federal Trade Commission, the Associated Credit Bureaus and Household International for joining us today to educate the subcommittees and the public on this important issue.

I look forward to learning today how we can improve enforcement of the statutes on the books and what else we in Congress as well as private industry and consumers can do to stop identity theft and the damage it has already done to consumers and businesses across America.

Thank you, Mr. Chairman.

Mr. TAUZIN. Thank you very much, Mr. Chairman.

I wanted to acknowledge that the ranking minority member, Mr. Markey, of our subcommittee is in an electricity hearing upstairs and has sent word that he apologizes for not being here. It does not mean that he is not deeply committed to resolving some of these problems with us here.

And the chair now recognizes any member who would like to make an opening statement.

Mr. Luther of Minnesota.

Mr. LUTHER. Thank you, Mr. Chairman.

Just briefly, I think most of us are very concerned about this issue and particularly the length of time that it takes to straighten out the record once the identity theft occurs. Obviously, we are all interested in seeing what can be done to shorten that period of time so people can get on with their lives. So anyone who has suggestions and recommendations along those lines, I hope you will share them.

Thank you, Mr. Chairman, for the hearing. It is a very important subject, and I appreciate your calling it.

Mr. TAUZIN. Thank you very much, Bill.

Mr. Towns will be coming. He is the ranking minority member of the subcommittee chaired by Mr. Oxley. He will be coming a little later. He is at a previous commitment.

Anyone on this side?

The author of the legislation that we will be discussing today, Mr. Shadegg.

Mr. SHADEGG. Thank you, Mr. Chairman; and I thank Mr. Oxley as well for holding this very important hearing today to discuss both an issue which is critically important to me, identity theft, and more important to me is the implementation of the legislation that we enacted last year, the Identity Theft and Assumption Deterrence Act which creates the basis for this hearing.

I am very pleased that you would schedule this hearing. I want to talk a little bit about the problem and then a little bit about what we discovered in trying to get the law enforced and implemented.

The issue of identity theft was brought to my attention by two of my constituents who were victims of identity theft. Bob Hartle and his wife experienced the devastation of identity theft firsthand when a convicted felon stole Mr. Hartle's identity and, using that stolen personal identification information, made purchases totaling $110,000. Using Mr. Hartle's identity, this individual obtained a Social Security card, a driver's license, bank accounts, credit cards and even life insurance in Mr. Hartle's name. He bought trucks, motorcycles, a mobile home, furniture and appliances.

Incredibly, he even obtained a security pass to a restricted area of Sky Harbor International and took advantage of Mr. Hartle's clean record to get around the Brady law and purchase handguns.

Mr. and Mrs. Hartle have had to spend a great deal of money to correct their credit ratings, indeed $15,000 to try to set the record straight. Because at the time these events occurred there were no criminal penalties for idebtity theft, the Hartles were left with virtually no remedy whatsoever. The individual was prosecuted for making false statements to purchase a handgun, and was sentenced to prison in 1995 and released earlier this year. But because there was no law at the time, he was not required to and did not make any restitution to the Hartles, the victims of the crime.

Today, as I think everyone in this room knows, identity theft has become the fastest-growing financial crime in America and indeed probably the fastest-growing crime of any kind in our society.

Arizona, in 1996, became the first State in the Nation to enact criminal penalties for identity theft. Since then, it has been joined by California, Colorado, Georgia, Kansas, Mississippi, Wisconsin and West Virginia. Other States, including New York, are similarly working to pass laws of this type.

The key to identity theft is that it prohibits the obtaining and the transfer of personal identification information. It used to be that you could prosecute people for credit card fraud or bank fraud or for bad checks, but that was all after the fact. What this law does, both the Arizona law and the laws enacted in other States and the law we were able to pass last year, is empower Federal law enforcement agencies to investigate the crime, apprehend the individual, and prosecute the individual before they cause the damage.

My colleague on the other side referred to the serious problem that is caused when someone's credit rating is destroyed because the crime has been effectuated. This law allows law enforcement

agencies to prevent the crime by stopping it before all of those consequences, all of the theft, all of the fraud occurs and someone's credit rating is completely destroyed.

I think that is the key to the law, and it is why this hearing is so important. The Federal Trade Commission, under the legislation we passed last year, was directed within 1 year of its enactment to establish a centralized complaint and consumer education service for the victims of identity theft, and I am sure that we will hear testimony about their efforts today. They are also required to log complaints from identity theft victims, to provide information materials to those victims and refer complaints to consumer reporting and law enforcement agencies.

I want to talk a little bit about what is happening now in the enforcement of the law and the problems that we are finding.

The two greatest obstacles that we are finding is, one, a lack of information amongst the public about the fact that this conduct is criminal and that they can report it as soon as it occurs.

Second, and this is more important and I hope our witnesses will discuss the issue, is confusion regarding jurisdiction. Many law enforcement agencies think, well, you have called me about an identity theft where your identity has been stolen, but we only handle bank fraud so we only handle the bad checks. No bad check has cleared yet. Then they turn that person away. Or someone comes in and says, have you had a credit card fraud? We are in charge of credit cards. We will handle it once you have some credit cards stolen.

The Arizona Attorney General's Office went out to a local law enforcement agency in Phoenix and, while waiting for an appointment, two individuals came to the window and complained and said, I want to complain about an identity theft which has occurred to me. In both instances, the policeman taking the complaint said they stole your identity and you are not the victim. Because, until this legislation passed, the theft was considered to have been committed against the credit card company or against the bank that wrote the check or against the individual who extended the credit, not the victim.

I am sure that we will hear from our victims that they really are the victim of the crime, but our laws prior to the passage of this legislation and the similar legislation in various States did not make the individual the victim. That illustrates one problem.

The second problem is the lack of awareness. The law enforcement officers, in this instance, the Arizona law had been in effect since 1996, the Federal law has been in effect for 6 months now, and this law enforcement agent said to the individual, you are not the victim. Obviously, they were the victim.

In an effort to educate the public about this crime and assist law enforcement in Arizona, I formed an Identity Theft Task Force, because victims kept coming to my office saying law enforcement is not helping us with this problem. Thirty-five members have shown up for the most recent meetings of this task force, and they include representatives from local police, County Attorney's Offices, the State Attorney General's Office and, I am very pleased to say, representatives in Phoenix from the FTC, FBI, the INS, the Secret Service, Postal Service, Social Security Administration and the U.S.

Attorney's Office along with representatives of the banking industry, the credit bureau industry and a number of private industry groups.

As a result of this task force, we have worked very hard to do two things. One is compile a list of the kinds of crimes that can be and are committed once somebody's identity has been stolen; second, to write a protocol so that law enforcement agencies will know how to handle these complaints when they come in. That protocol is in its final draft form. The Arizona Attorney General's Office and Maricopa County Attorney's Offices have worked on it, and I am very pleased to say that it is moving forward.

In the absence of that protocol what is happening in the enforcement of this law is confusion. Agencies don't know which agency has jurisdiction.

And just to give you a quick anecdote. During the last task force meeting, they explained that someone comes in to the Phoenix Police Department and they say, my identity has been stolen. They then begin to list the credit cards that may have been created and the bank accounts that may have been opened and the other credit which may have been established all across the country, a credit card issued in Delaware or a bank account established in perhaps Minnesota. The law enforcement agencies in Arizona say, how in the world do we have jurisdiction over this crime and how can we get the resources to enforce this crime?

Because the nature of the crime is the theft of an individual's identity, I argue that at least legal jurisdiction for prosecution of that crime is wherever that person lives. That creates a huge resource problem for the local law enforcement agencies.

I do believe that the Federal Trade Commission can do a great deal of good in this area. I commend them for their efforts. And, again, I commend both chairmen of these subcommittees for holding this hearing so we can move forward on enforcement of this important law.

Mr. TAUZIN. Thank you. Both of us were commenting on how much of an effort you have been responsible for and how much the victims across America should be indebted to your dedication and work in this area.

Mr. SHADEGG. Thank you.

[The prepared statement of Hon. John Shadegg follows:]

PREPARED STATEMENT OF HON. JOHN B. SHADEGG, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF ARIZONA

Thank you Mr. Chairman. I am pleased that the Subcommittees on Finance and Hazardous Materials and Telecommunications, Trade and Consumer Protection have combined efforts today to discuss an issue that is very important to me—identity theft.

Identity theft occurs when stolen personal information is used to establish false credit, open checking accounts, apply for loans, file for bankruptcy, and run up thousands of dollars in debt by someone other than the individual whose identity was stolen. Victims are left to clean up the mess, settle thousands of dollars in debt, and reestablish their credit.

This problem was first brought to my attention by two of my constituents, Bob and JoAnn Hartle of Phoenix, Arizona, who, being victims of identity theft, were instrumental in passing the first state law in the nation making identity theft a crime and assisted me in passing H.R. 4151, the *Identity Theft and Assumption Deterrence Act*.

Mr. and Mrs. Hartle experienced the devastation of identity theft first hand when a convicted felon stole Mr. Hartle's identity and, using this stolen personal identification information, made purchases totaling more that **$110,000.** With Mr. Hartle's identity, this individual obtained a Social Security card, driver's license, bank accounts, credit cards, and life insurance in Mr. Hartle's name. He bought trucks, motorcycles, a mobile home, furniture, and appliances.

Incredibly, he even used Mr. Hartle's identity to obtain Federal Aviation Administration security clearance to Sky Harbor International Airport in Phoenix. He used Mr. Hartle's military service in Vietnam to get a federal home loan and even took advantage of Mr. Hartle's clean record to get around the Brady Law and purchase handguns.

Mr. and Mrs. Hartle have spent over $15,000 of their own money—and over four years of their lives—re-establishing their good credit and reclaiming Bob's identity. Because at the time these events took place there were no criminal penalties for identity theft, the Hartles were left with virtually no remedy. The criminal who victimized them was prosecuted for making false statements to procure firearms. He was sentenced to prison in 1995 and released earlier this year. Most importantly though, he was not required to, and therefore did not make any restitution to the innocent victims of his outrageous conduct, the Hartles.

Tragically, the Hartles' story is far from unique. Today, identity theft has become the fastest growing financial crime in America and one of the fastest growing crimes of any kind in our society. Thousands of people are victimized every day. A single national credit bureau reported that over two-thirds of the complaints it received in 1997 involved identity theft—a total of 300,000 complaints in just one year. Cost to individual victims, financial institutions and taxpayers from identity theft have skyrocketed in recent years to almost $2 billion dollars annually.

In 1996, my state of Arizona became the first state in the nation to enact criminal penalties for identity theft. Since then, California, Colorado, Georgia, Kansas, Mississippi, Wisconsin and West Virginia have enacted similar laws making this conduct criminal. Several other states, including New York, are currently working to pass state identity theft laws.

In response to the Hartle's story and the growing number of identity thefts across the country, I introduced H.R. 4151, the *Identity Theft and Assumption Deterrence Act,* in the 105th Congress to make identity theft a federal crime. And, after introducing this legislation last year, literally hundreds of constituents came forward to tell Members of Congress their stories of victimization, including dozens of congressional staff members here on Capitol Hill.

H.R. 4151 passed the House of Representatives by voice vote on October 7, 1998, and subsequently received unanimous consent from the Senate and was signed into law on October 30, 1998.

This new federal identity theft law prohibits the transfer and use of personal identification information—such as a person's name, address, or social security number—to acquire an individual's identity. This empowers federal law enforcement agencies to investigate, apprehend and prosecute criminals *before* they can use an individual's stolen identity to acquire credit cards, checking accounts, home loans, purchase vehicles, furniture, appliances or handguns or otherwise cause irreparable damage to victims.

Identity thefts range from individual instances involving small and large amounts of money, like the Hartle's, to organized, professional crime rings operating in multiple states and stealing hundreds of thousands of dollars. One such crime ring, using a fictitious home improvement business as a front, established a credit bureau account and used its computer link to download roughly 500 credit reports. With this personal financial information, the crime ring stole more than *$250,000.*

The identity theft law imposes penalties of up to 15 years imprisonment for federal identity theft crimes and increases penalties to 20 years for identity theft crimes associated with drug trafficking offenses or any violent crime. Because H.R. 4151 created a new crime under the federal fraud statute, victims of identity theft can now seek restitution for expenses incurred to reestablish their credit as well as compensation for legal and court fees.

Finally, H.R. 4151 directed the Federal Trade Commission (FTC), within one year of enactment, to establish a Centralized Complaint and Consumer Education Service for victims of identity theft. Specifically, the FTC is required to log complaints from identity theft victims, provide informational material to victims, and refer complaints to the appropriate consumer reporting and law enforcement agencies.

The FTC is currently working to establish a toll free number for identity theft victims, to create a separate consumer complaint database for identity thefts and to develop consumer educational materials. In an attempt to streamline the information included in these educational materials, the FTC is drawing from existing

materials provided by a variety of federal agencies as well as new information regarding identity theft to create a more thorough and up-to-date set of materials.

In the interim, the FTC has taken steps to assist identity theft victims right now, including training current consumer complaint phone counselors to facilitate identity theft inquiries. In addition, modifications have been made to the existing database to log identity theft complaints until a permanent database is in place and current educational materials available to consumers have been expanded to address identity theft. Finally, the FTC anticipates that in the coming weeks, the consumer complaint website (located at www.consumer.gov) will have an identity theft page added to provide information and links to other federal law enforcement agencies.

It has come to my attention that the two greatest obstacles to enforcing the laws in this area and deter identity theft are a lack of awareness and confusion regarding jurisdiction. Victims are unsure of their options for repairing their damaged credit ratings and eliminating the accrued debt. Likewise, law enforcement is often unfamiliar with existing state, and now federal laws that provide them with the ability to actively investigate and prosecute identity thefts. Although Arizona's identity theft law has been in place since 1996, and now has the backing of the federal law, both victims and law enforcement agencies from around the state are still experiencing difficulty and confusion in how to handle complaints of identity thefts.

In an attempt to further educate the public about this crime and assist law enforcement, earlier this year I formed an Identity Theft Task Force. This thirty-five member task force includes representatives from local police, county attorney's and state attorney general's offices. In addition, staff members from the local FTC, FBI, INS, Secret Service, Postal Inspectors, Social Security and U.S. Attorney's Office, along with banking and private industry groups participate in the task force.

As a result of this effort, the Task Force has compiled a list of the different types of crimes that can be committed once someone's identity is stolen and a protocol for handling identity theft complaints is being written. This will assist law enforcement in determining the appropriate jurisdiction for crimes associated with identity theft. The Arizona Attorney General's Office, the Maricopa County Attorney's Office and the Secret Service are currently working to compile an educational booklet for consumers and agencies.

In the absence of a protocol for handling identity theft complaints, victims are being turned away by law enforcement because the agencies do not understand the law or how to process complaints. The Identity Theft Task Force is continuing to meet regularly and I am confidant that opening the lines of communication between consumers, law enforcement and private industry is the most effective method to fully enforce the state and federal identity theft laws and assist victims with reestablishing their credit and their good name.

I commend Chairman Oxley and Chairman Tauzin for holding this hearing to inform both Members of Congress and the public about the pervasiveness of identity theft and the efforts underway by federal and state agencies and industry to combat this crime. Furthermore, I hope the witnesses can elaborate on the obstacles that still exist which effectively prevent the prosecution of instances of identity thefts. I would like to thank both the Associated Credit Bureaus and the Federal Trade Commission for their efforts to implement the new federal identity theft law and acknowledge their initiatives. I look forward to hearing their testimony on the progress of this program and their thoughts on the frequency of identity theft based on consumer complaints to date.

Thank you and I yield back the balance of my time.

Mr. TAUZIN. Any other members wish to make an opening statement?

Dr. Ganske, you are recognized.

Mr. GANSKE. Mr. Chairman, I am interested in learning about identity theft and what the FTC is doing about it. My understanding is that we will hear some personal examples today of this problem, and I think it is commendable that you are holding a hearing on this to draw public attention to this problem, and I thank you.

Mr. TAUZIN. Thank you, Mr. Ganske.

Anyone else for an opening statement?

Then the Chair is pleased to yield to Chairman Oxley to introduce the panel. As he introduces you, if you will come forward and take your seats.

Mr. Oxley.

Mr. OXLEY [presiding]. Thank you, Mr. Chairman.

Let me first introduce Mr. Robert Anderson from Mineral, Virginia; and Ms. Jodie Bernstein, the Director of the Bureau of Consumer Protection at the Federal Trade Commission; Mr. Charles A. Albright, Chief Credit Officer from Household International; and Mr. D. Barry Connelly, President of the Associated Credit Bureaus here in Washington.

Thank you, all of you, for appearing.

Mr. Anderson, we will begin with you.

**STATEMENTS OF ROBERT ANDERSON, MINERAL, VIRGINIA; JOAN Z. BERNSTEIN, DIRECTOR, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION; CHARLES A. ALBRIGHT, CHIEF CREDIT OFFICER, HOUSEHOLD INTERNATIONAL, INC.; AND D. BARRY CONNELLY, PRESIDENT, ASSOCIATED CREDIT BUREAUS, INC.**

Mr. ANDERSON. I thank you for the opportunity to share my story with you. I have heard some of these kinds of stories before, particularly with credit card and bank account theft; and I think mine is just a little bit different, as you will see, in that the perpetrator hasn't stolen anything tangible from me other than my credit rating. All of the thefts have been from other places, businesses primarily.

Basically everything I have to say is based on my own documentation, which is extensive; and I am glad that early on I started documenting, because it would probably be 15 years instead of 5 years if I had not.

I don't know statistically how identity theft normally begins, but in my case it was not lost credit cards, it wasn't a lost or stolen driver's license, and it was not something stolen from a checking account or a mailbox. Rather, it was a number from a supposedly very protected system of records, my Social Security account number.

At the beginning, the person responsible for this found a way, and I don't know to this date just how, to go into five different Social Security offices in California and get my number and I believe in each case probably not only the number, but little bits and pieces of identity to go with it. It wasn't immediately obvious that anything was happening. Except that in 1994 I got called into a Social Security office regarding a disability claim for somebody with a name very similar to mine, but not me. When I visited the office, they said, yes, it appears there has been an enumeration problem; and we are going to correct it. At that point, I thought the problem was solved.

Well, several months later, getting into 1995, I found strange things happening with my credit reports. Just really casual applications for credit cards or lower balance credit cards, whatever, were turned down. And in almost every case, I would receive a notice from the bank involved that I had collections and foreclosures on my credit report. Of course, since I have never had a collection or foreclosure in my life, I immediately tried to find out what that was all about.

When I pulled the reports, and that was an effort in itself, it took three attempts before one of the credit reporting agencies even re-

sponded to me, and even then I had a lot to learn. I had to learn to play the game in that the format of whether I needed to send $8, whether I needed to write it on yellow paper or green paper, what have you.

Once I learned to play the game, I was able to pull my reports from all three of the credit reporting agencies. When I did, lo and behold, there were collections and foreclosures at that point in time based on telephone service, cellular and interstate telephone service from a cellular company and Pacific Bell.

Well, I immediately contacted the provider of that derogatory information and their collection agency and explained to them that I had a Social Security number fraud problem and that the accounts didn't belong to me, that I never had telephone service in California, that I had never had a cellular phone in California.

I was given assurance that it would be taken care of. At that point, it was TRW that I was dealing with; and nothing happened. So when I saw that nothing was happening, 6 or 8 weeks later I decided I better do something about it.

And, just thinking it through, that I had witnessed a theft of interstate telephone communications, I wrote a letter to the FBI in California. I was contacted subsequently by the Special Agent in Charge who said, yes, this sounded like it was a problem, but it didn't rise to the level of things that they could investigate.

Basically, I was told by the FBI that, in California at least, they really couldn't get into cases like this or I guess any kind of a personal theft thing unless it rose to the level of $250,000. In my case we are talking about thousands of dollars, not anything like that.

So armed with that information, I started with Social Security. I contacted the Office of Inspector General and their hot line, and I advised them of what was happening and of the information that I had from the Social Security Administration and they put me in the queue. After months and months of some conversation but nothing happening, I got pretty adamant with the Inspector General's Office, and I found out that basically, was that they could not do anything because of the burden of the backlog of beneficiary theft, that is, checks actually taken out of mailboxes were keeping them too busy and that they didn't quite know what to do with me.

At that point I decided I probably better get after the credit reporting agencies and start focusing on the things that I could do with the Fair Credit Reporting Act.

I again pulled my credit reports. Now there was even more substantial bad derogatory credit information, and it was clear that the person doing this had obtained a little more of my identity. I don't know how. I have to suspect since one credit report was totally merged, that is, I know this person's workplaces, I know this person's addresses, so on and so forth, I have to assume that that person probably knows the same thing about me if he pulled the same credit report. I have to assume that risk.

I pulled over 20 credit reports from the crediting agencies over the past 3 years, and I have disputed virtually every one of them. I guess only recently, and I will explain why a little bit more, the person got into use of medical services; and that actually helped me.

But, after disputes, I was able to pretty well clear up one of the three credit reporting agencies. The other one still had these computer problems with this merged report. And although they took out the addresses and some things of the other person, they put the same computer numbers, Los Angeles file numbers and things on my report and put my name and address on the cover of it; and that is where that stands today. So the other person is indeed off that credit report, but the information is not.

The third one generally refused to do anything. They said that they had contacted the likes of the telephone companies in California, and department stores were a favorite of this person. And that they had been advised, because a valid Social Security number had been presented, they could not do much for me.

Now this was after I had sent these people copies of a letter that I had from Social Security advising them that I was a fraud victim. This is after I had them place statements on my credit reports over 3 years that I didn't want any credit to be granted to anybody because I was a fraud victim and I was to be contacted, et cetera, if that was the case. Yet the third CRA still wouldn't do anything and to this day still won't do anything about the disputed and disputed and disputed information that clearly emanates from California, that clearly fits the mold of the fraud that occurred, and it is frustrating I guess is the best way to state that.

A major breakthrough in starting to get something going was that the person started using hospitals and medical facilities. Just about every night at dinner time we would get a call and it would be from a collection agency wanting to know when I was going to pay them for the surgery that was done and the likes of this. It was appalling to me then and still is that a hospital or a doctor could perform surgery on somebody and not even know who they were operating on, and that seems to be the case.

Similarly, with the department stores, that fit the same category. These are the kinds of things that would happen. There is a Mervyns store out in California. The person would walk in, open an account, charge right away $500 or $600 worth of merchandise; and 2 or 3 months later I would get the call at dinner time. The person has never tried, as far as I know, to get into my bank accounts, has never tried to steal money from myself, but it has always been consumer, department store, or medical fraud.

In my opinion, the laws seem pretty clear. I have read the Fair Credit Reporting Act. I am somewhat familiar with the Criminal Code. There are a number of laws that seem to be out there, and I really do welcome the one criminalizing the one with the use of identity with the smaller dollar amount that came out last year, but the problem is finding somebody that thinks that the theft of your identity is worth a quarter of a million dollars or whatever standard they have set to do something about it. If there is anything that can be done with setting standards, I think it could be very helpful to people such as myself.

In the case of the victim, I will be quite honest with you, I think I could have solved this real quickly if I was wealthy. Basically, the attorneys that I talked to told me to get a high-profile attorney. I guess that means if you are a victim of identity theft and you can afford the likes of an F. Lee Bailey or a Johnny Cochran, you can

probably solve the problem. But I found it extremely difficult to find attorneys that were subject matter knowledgeable and that were willing to take the case on a modest fee or some other basis, particularly in my case when the actual damages that would go into the lawsuit are not huge, $50,000 would be my guess at this point. The whole thing in my case is going to be punitive damages.

And what is my identity worth? I don't know. I think that is one of the major things that can be done to help victims, is to set some standard that this is worth as much as a diamond or $250,000 or whatever, so that the people that are responsible for prosecuting and enforcing the laws can do something about it.

As far as the credit reporting agencies go, I don't know. I think the FCRA is a real good document. I think this covers all of the bases. But what I have seen in terms of foot dragging, requiring notification time after time after time again of a moving target which, by the way, by the time they correct has moved to another place and you have another problem, that is hard to deal with.

I am advised by attorneys that the legal process is no better. That going into court, first of all, will probably, this is under 15 U.S. Code now, probably results in a modest award. It has in the past in some cases, but that award is going to be appealed by a throng of lawyers, and the reality is that the case is going to be in court for years. I don't know what to do about that one. I don't know where we set a standard.

And I have probably run up my 5 minutes right there. That is about the story. I am looking for any help I can get, and I welcome the opportunity to sit here and tell you the story.

[The prepared statement of Robert Anderson follows:]

PREPARED STATEMENT OF ROBERT ANDERSON

In Mid 1994 I became aware of a problem with my Social Security Number and also experienced denial of very routine credit due to reported "collections and foreclosures." I have never had a collection nor foreclosure against myself.

In August of 1994 I visited a Social Security District Office in Baltimore, Maryland, and was advised that SSA records showed my SSN as belonging to a person with a similar name, but not myself. I was told that the problem would be corrected.

During the same period I began to experience unusual reactions from creditors, and was advised several times that this was due to "Collections and foreclosures."

Virtually all of my investments were in Real Estate. Since I was now a widower and an early retiree, I decided to sell my primary residence, reduce and eliminate real estate debt, and move to another property I already owned. In the process I applied for mortgage refinance credit and found that I now had credit problems. My credit reports in December 1995, showed collections and foreclosures on telephone service in California occurring from late 1994 through 1995. This derogatory information delayed and made my Real Estate transactions either very difficult or impossible thus depriving me of significant financial leverage.

I obtained some information regarding the Fair Credit Reporting Act, and requested copies of my consumer credit report from all three of the major Credit Reporting Agencies (CRA'S). I was advised that I needed to get the individual collection agencies to contact the CRA in order to remove the derogatory information and was given contact information. The agencies involved and particularly, Pacific Bell Telephone would not delete the harmful information from my reports since it had been verified by someone using my SSN.

My mortgage processor advised me to contact Social Security and obtain a statement that my SSN was being used fraudulently. I did so, and received a letter from the SSA District Office stating that my SSN had been issued to another person on five different occasions. All SSN issuance's were in the Pomona/Glendora area of California, and I was even provided with a local address in California, reported as belonging to myself.

When I moved and applied for a driver's license (which uses SSN), I was delayed and questioned by a motor vehicle inspector as to whether I had ever lived in, or had a record in California. Recognizing that this had become a serious problem requiring resolution I escalated my efforts.

At this point, I had a name, address and other information about the person in California, and decided that I must attempt to stop their damaging actions.

Telephone calls to local law enforcement agencies in California did no good. I was told that since I live in another State, I must file a complaint with my local authorities. The State Police told me that this appeared to be a Federal matter and that I should contact FBI. I wrote to the FBI in California and advised that identity fraud had occurred involving interstate telephone services. The special agent in charge called me and advised that unless the dollar amount of the fraud exceeded $250,000, they could do nothing. I contacted the Social Security Office of Inspector General Hotline and attempted to file a complaint in order to obtain some sort of police report number. I was initially told that SSA had such a backlog of beneficiary theft (checks) that they could do nothing. After three years of telephone calls and endless letter writing, I still have not reached resolution with SSA. Only after Congressional intervention did I receive indications of help from SSA.

Thus began a four year long nightmare of credit problems. The perpetrator was apparently knowledgeable enough not to apply for credit cards, commit postal fraud, nor directly attack my personal accounts. Instead, he began victimizing Department stores by applying for revolving credit, immediately purchasing to the limit, and disappearing. I would receive a call from some collection agency and would recite my story of Social Security Number theft and identity fraud. In some cases, such as Montgomery Wards, research performed indicated the existence of someone in California and the matter was removed from my credit report. In other cases, such as Target, and Mervyns, the information was never corrected; and I still receive calls from collections agencies. Both Target and Mervyns were advised of the SSN problem and fraud, yet chose to ignore that information.

The California fraud now began to use Medical facilities in California, using my SSN for billing. I received phone calls, letters of collection, and collection agency actions from two Hospital groups, an ambulance service and radiology centers. One surgeon sent me a statement that he performed surgery upon myself (I have never had surgery). It was clear that the Medical facilities did not know who they were treating. I obtained legal counsel and one of the hospitals corrected and wrote off at least $6,000 in charges, but only after threat of lawsuit. The others remain a problem and still appear on some of my credit reports. I have been unable until just recently to reduce the interest rates of my credit accounts due to the fraud. My children are routinely offered credit at 6% while I have been saddled with 18% credit for three years.

The CRA's were another story. I notified all that was I was a fraud victim, and disputed the erroneous information on their reports. I asked that statements be put on my report to advise creditors of the fraud and not to grant credit without my permission. The CRA's responded variously, but I found that as soon as I could correct and dispute one item, frequently more bad credit information would be added. At one point a credit report completely merged my personal and credit information with that of someone in California, thus providing me with addresses, places of work, credit history and other information. When I disputed the information, the report was corrected to reflect only my name and address but still contained all information on two different persons, including the CRA coding information. I requested and disputed my credit reports every 90-180 days and disputed in writing all erroneous information. Although this is finally beginning to result in an accurate report, one of the major CRA's still willfully refuses to remove damaging erroneous information. That CRA has been provided multiple copies of letters from SSA which document myself as a fraud victim.

There seem to be more than adequate Federal laws in existence to cover my situation. Title 15, USC 1681, the Fair Credit Reporting Act, provides both for theft and fraudulent use of SSN's and for willful failure of credit reporting agencies to protect consumers by correcting fraudulent information. The Federal Criminal Code, Title 18, USC 1028, also appears to make the SSN use a federal offense. I expect there are other related laws.

The problem I have experienced is the tremendous difficulty in causing someone to prosecute and/or enforce the laws unless there is a large amount of money involved. This raises the questions in my mind: What is the value of one's identity? What is the value of ones credit worthiness? What is the price to be paid for the stress, suffering and personal damage to a victim? This applies not only to law enforcement agencies, but to attorneys as well. My experience has been that where an Attorney can choose between a personal injury automobile accident case, and an

identity theft case, the personal injury case wins hands down. I am advised that should one lose a Federal Civil case against a CRA, the CRA may charge all legal fees to the plaintiff. I also am told that the CRA will most certainly appeal should a judgement against them be rendered, and that the history of existing cases indicates years of litigation in each case. After two aborted attempts to pursue litigation against a CRA have been sidetracked due to the complexities of my case, I still pursue Federal Civil Court action.

Mr. TAUZIN. Mr. Anderson, we deeply appreciate it.

Actually, we did not put a timer on you. We thought after all these years, you ought to be able to say whatever you wanted to say for as long as you wanted to say it. Thank you, Mr. Anderson.

Ms. Bernstein.

**STATEMENT OF JOAN Z. BERNSTEIN**

Ms. BERNSTEIN. Thank you very much, Mr. Chairman, all three chairmen. Thank you very much for the opportunity to be with you today at this very important hearing on this subject that the Commission cares very deeply about.

Before I start, as your practices are, I think, Mr. Chairman, our full statement will be accepted for the record; and I will just summarize briefly for you this morning the steps that the Commission has already undertaken, what our plans are for the future.

I would like to thank Mr. Shadegg particularly for his leadership in this area in recognizing the capacity of the FTC that has been working in the area of handling consumer complaints over the last couple of years especially.

Our hope is, in welcoming the authority that the committee and the Congress gave us, is that it will result in a better system for people like Bob Anderson who have suffered such grave damage to their reputations and to the loss of their identity. Hopefully, as we finish the implementation of this and the Fair Credit Reporting Act amendments, it will result in a better system.

Just to focus on the statute itself, the Identity Theft Assumption and Deterrence Act, and as you pointed out in your statement, the act requires the FTC to establish procedures to do three things: to log the receipt of complaints by victims of identity theft; to provide victims of identity theft with informational materials; and, three, to refer complaints to appropriate entities, including major national credit bureaus and law enforcement agencies.

We intend to meet your deadline of October 1 to have these procedures in place. They are already under way.

So the way we view our role, it is largely as a coordinator, to serve as a central point of contact and the source of information for victims and to manage that information to be shared with the various agencies in its support of law enforcement.

So what we have done specifically is we have a plan to establish an 800 number. It is already under way. We have already reserved a number which is a pretty good one, 877-I-D-theft—it has been reserved, but it has not been implemented just yet—in order to take complaints from consumers and provide them with information as to what to do about it. I think that is a critical role for us.

We are also planning, and it is also under way, a data base. It is built on the other data bases that the Commission has already established so that the information can be available across the country out of the data base. It will help law enforcement, particu-

larly. If I haven't stressed that enough, the coordinating function between us as a repository of information and criminal law enforcement across the country in the Federal agencies will be critical.

And perhaps as important as the other functions are the education or informational function. We have started on that, and we issued a consumer alert in April that is on identity crisis, what to do if your identity is stolen. And the first thing to do is to give specific information as to where to report initially an episode of identity theft. These are available. Copies are available with me here today.

This back page, Chart Your Course of Action; and it is helpful in identifying what you ought to do initially if you have been a victim of identity theft. It is to help victims begin to cope with this problem.

What have we done in addition to these steps? We have trained our consumer response center counselors, and we have them in place to handle other consumer problems, and we have added a number to that staff to recognize ID complaints and assist victims right away if and when they call up. We already have numbers in place for that.

We have modified our existing data base to track basic information on the ID theft calls that we are already receiving. As I said, we have issued consumer information already. We are publicizing it as broadly as we can, this consumer information, and through media coverage of the consumer information.

Within a couple of weeks we are about ready to launch a web page that will be dedicated entirely to identity theft, and it will be built on www.consumer.gov, which is a page that we took the initiative on and has 61 Federal agencies coordinating. I am proud of it because, for the first time, a consumer can get information from the Federal Government without knowing what the acronym is for the agency, and I think that is a real breakthrough. So we will be building on that experience.

Just this week we held a conference with 16 Federal agencies to begin to get them to be aware of the need to coordinate this information and to foster law enforcement as best we can. The National Association of Attorneys General also attended that. We want them to coordinate with us as we begin to develop the tools for consumers so that we are getting from consumers the information that they need, that law enforcement needs in order to bring rapid enforcement in this area.

On a related subject, I would add one more point, because this is important. It was stated in the written testimony of the Commission, this week the Commission—just yesterday, they authorized us to file a complaint in Federal court that for the first time attacked the process known as pretexting. Pretexting is people who, I guess in lay language, lie about who they are to obtain very sensitive financial information to be used by third parties without the authorization of you, the consumer, whose material it is.

We filed a case in Colorado yesterday naming Touchtone Information, a company which we believe plays a significant role in this business, to attack under section 5 of the FTC act the Commission's existing authority to attack deceptive and unfair practices for two things, the lying and the passing on of the information.

We will be happy to keep the committee advised as to the course of that litigation. I have with me today copies of the complaint as well as the majority and dissenting statements of the Commission for your information.

I do want to say that others here at the table have been very helpful and cooperative in terms of our consumer education efforts. We will need the private sector as well as the government agencies to carry out the task.

Again, I thank the committee for the opportunity to be with you today.

[The prepared statement of Joan Z. Bernstein follows:]

PREPARED STATEMENT OF JOAN M. BERNSTEIN, DIRECTOR, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION

Mr. Chairman Tauzin, Mr. Chairman Oxley, and members of the Subcommittees, I am Jodie Bernstein, Director of the Bureau of Consumer Protection, Federal Trade Commission ("FTC" or "Commission").[1] I appreciate the opportunity to present the Commission's views on the important issue of financial identity theft.

In my remarks today, I will discuss the increasingly common problem of identity theft, the role of the FTC in addressing this problem under the recently enacted Identity Theft and Assumption Deterrence Act[2], and the steps the Commission is taking to aid consumers who become identity theft victims. I will also briefly address one of the notable ways in which identity theft can occur in the financial services industry—"pretexting," *i.e.*, obtaining private financial information from banks and others under false pretenses.

I. IDENTITY THEFT: THE PROBLEM

Identity theft occurs when someone uses the identifying information of another person—name, social security number, mother's maiden name, or other personal information—to commit fraud or engage in other unlawful activities. For example, an identity thief may open up a new credit card account under someone else's name. When the identity thief fails to pay the bills, the bad debt is reported on the victim's credit report. Other common forms of identity theft include taking over an existing credit card account and making unauthorized charges on it (typically, the identity thief forestalls discovery by the victims by contacting the credit card issuer and changing the billing address on the account); taking out loans in another person's name; writing fraudulent checks using another person's name and/or account number; and using personal information to access, and transfer money out of, another person's bank or brokerage account. In extreme cases, the identity thief may completely take over his or her victim's identity—opening a bank account, getting multiple credit cards, buying a car, getting a home mortgage and even working under the victim's name.[3]

Identity theft almost always involves a financial services institution in some way—as a lender, holder of a bank account, or credit card or debit card issuer—because, as the bank robber Willie Sutton observed, that is where the money is. Identity theft involving financial services institutions, furthermore, is accomplished through a wide variety of means. Historically, identity thieves have been able to get the personal information they need to operate through simple, "low-tech" methods: intercepting orders of new checks in the mail, for example, or rifling through the trash to get discarded bank account statements or pre-approved credit card offers. Sometimes, identity thieves will try to trick others into giving up this information. As discussed in more detail below, one way in which identity thieves do this is by "pretexting," or calling on false pretenses, such as by telephoning banks and posing as the account holder. In other cases, the identity thief may contact the victim directly. In one recent scheme, fraud artists have reportedly been preying on consumers' fears about Year 2000 computer bugs; a caller, for example, represents that he

[1] This written statement represents the views of the Federal Trade Commission. My oral presentation and response to questions are my own, and do not necessarily represent the views of the Commission or any Commissioner.

[2] Pub. L. No. 105-318, 112 Stat. 3007 (1998).

[3] In at least one case, an identity thief reportedly even died using the victim's name, and the victim had to get the death certificate corrected. Michael Higgins, *Identity Thieves,* ABA Journal, October 1998, at 42, 47.

or she is from the consumer's bank and tells the consumer that the caller needs certain information about the consumer's account (or needs to transfer money to a special account) in order to ensure the bank can comply with Year 2000 requirements.[4]

Other methods of identity theft may involve more sophisticated techniques. In a practice known as "skimming," identity thieves use computers to read and store the information encoded on the magnetic strip of an ATM or credit card when that card is inserted through either a specialized card reader or a legitimate payment mechanism (*e.g.*, the card reader used to pay for gas at the pump in a gas station). Once stored, that information can be re-encoded onto any other card with a magnetic strip, instantly transforming a blank card into a machine-readable ATM or credit card identical to that of the victim. In addition, the increased availability of information on the Internet can facilitate identity theft.[5]

For individuals who are victims of identity theft, the costs can be significant and long-lasting. Identity thieves can run up debts in the tens of thousands of dollars under their victims' names. Even where the individual consumer is not legally liable for these debts,[6] the consequences to the consumer are often considerable. A consumer's credit history is frequently scarred, and he or she typically must spend numerous hours sometimes over the course of months or even years contesting bills and straightening out credit reporting errors. In the interim, the consumer victim may be denied loans, mortgages, and employment; a bad credit report may even prevent him or her from something as simple as opening up a new bank account at a time when other accounts are tainted and a new account is essential. Moreover, even after the initial fraudulent bills are resolved, new fraudulent charges may continue to appear, requiring ongoing vigilance and effort by the victimized consumer.

Although comprehensive statistics on the prevalence of identity theft are not currently available, the available data suggest that the incidence of identity theft has been increasing in recent years. The General Accounting Office, for example, reports that consumer inquiries to the Trans Union credit bureau's Fraud Victim Assistance Department increased from 35,235 in 1992 to 522,922 in 1997,[7] and that the Social Security Administration's Office of the Inspector General conducted 1153 social security number misuse investigations in 1997 compared with 305 in 1996.[8]

## II. THE FEDERAL TRADE COMMISSION'S AUTHORITY

### *A. Overview*

The FTC's mission is to promote the efficient functioning of the marketplace by protecting consumers from unfair or deceptive acts or practices and increasing consumer choice by promoting vigorous competition. The Commission's primary legislative mandate is to enforce the Federal Trade Commission Act ("FTC Act"), which prohibits unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce.[9] With certain exceptions, the FTC Act provides the Commission with broad civil law enforcement authority over entities engaged in or whose business affects commerce,[10] and provides the authority to gather information about

---

[4] FEDERAL TRADE COMMISSION, Y2K? Y2 CARE: PROTECTING YOUR FINANCES FROM YEAR 2000 SCAM ARTISTS (Consumer Alert, March 1999).

[5] *See, e.g.,* FEDERAL TRADE COMMISSION, INDIVIDUAL REFERENCE SERVICES: A REPORT TO CONGRESS (December 1997) (examining computerized databases or "look-up services" that disseminate personally identifiable information on individuals, often through on-line access). With the FTC's encouragement, members of the individual reference services industry have adopted voluntary guidelines, effective December 31, 1998, limiting the availability of certain types of personal information.

[6] The Fair Credit Billing Act, 15 U.S.C. § 1601 *et seq.* and the Electronic Fund Transfer Act, 15 U.S.C. § 1693 *et seq.* limit consumers' liability for fraudulent transactions in connection with credit and debit cards, respectively.

[7] Calls to this department included "precautionary" phone calls, as well as calls from actual fraud or identity theft victims.

[8] U.S. GENERAL ACCOUNTING OFFICE, IDENTITY FRAUD: INFORMATION ON PREVALENCE, COST, AND INTERNET IMPACT IS LIMITED (May 1998). The Social Security Administration attributed the increase in investigations, in part, to the hiring of additional investigators.

[9] 15 U.S.C. § 45(a).

[10] Certain entities such as banks, savings and loan associations, and common carriers as well as the business of insurance are wholly or partially exempt from Commission jurisdiction. *See* Section 5(a)(2) of the FTC Act, 15 U.S.C. § 45(a)(2), and the McCarran-Ferguson Act, 15 U.S.C. § 1012(b).

such entities.[11] The Commission also has responsibility under approximately forty additional statutes governing specific industries and practices.[12]

Among the Commission's statutory mandates of particular relevance here are the Fair Credit Billing Act and Fair Credit Reporting Act, which provide important protections for consumers who may be trying to clear their credit records after having their identities stolen. The Fair Credit Billing Act, which amended the Truth in Lending Act, provides for the correction of billing errors on credit accounts and limits consumer liability for unauthorized credit card use.[13] The Fair Credit Reporting Act ("FCRA") regulates credit reporting agencies and places on them the responsibility for correcting inaccurate information in credit reports.[14] In addition, the FCRA limits the disclosure of consumer credit reports only to entities with specified "permissible purposes" (such as evaluating individuals for credit, insurance, employment or similar purposes) and under specified conditions (such as certifications from the user of the report).[15]

*B. The FTC's Activities With Respect to the Financial Services Industry and Financial Privacy*

The Commission has extensive experience in addressing consumer protection issues that arise in the financial services industry, involving, for example, the use of credit cards, lending practices, and debt collection.[16] The Commission also provides consultation to Congress and to the federal banking agencies about consumer protection issues involving financial services. The Commission periodically provides comments to the Federal Reserve Board regarding the Fair Credit Reporting Act, and the implementing regulations for the Truth in Lending Act, the Consumer Leasing Act, the Electronic Funds Transfer Act, and the Equal Credit Opportunity Act.[17]

In addition, The FTC has taken an active role in addressing a range of issues involving consumer privacy, including the privacy of personal financial information. Thus, for example, the Commission has recently reported to or testified before Congress and/or held public workshops on online privacy, individual reference services, pretexting, financial privacy, and the implications of electronic payment systems for individual privacy.

*C. The FTC's Role in Addressing Identity Theft*

As an outgrowth of its broader concern about financial privacy, the Commission has been involved in the issue of identity theft for some time. In 1996, the Commission convened two public meetings in an effort to learn more about identity theft, its growth consequences, and possible responses. At an open forum held in August 1996, consumers who had been victims of this type of fraud, representatives of local police organizations and other federal law enforcement agencies, members of the

---

[11] 15 U.S.C. § 46(a).

[12] In addition to the credit laws discussed in the text, the Commission also enforces over 30 rules governing specific industries and practices, *e.g.,* the Used Car Rule, 16 C.F.R. Part 455, which requires used car dealers to disclose warranty terms via a window sticker; the Franchise Rule, 16 C.F.R. Part 436, which requires the provision of information to prospective franchisees; and the Telemarketing Sales Rule, 16 C.F.R. Part 310, which defines and prohibits deceptive telemarketing practices and other abusive telemarketing practices.

[13] 15 U.S.C. §§ 1601 *et seq.*

[14] 15 U.S.C. §§ 1681e, 1681i .

[15] 15 U.S.C. § 1681-1681u.

[16] For example, in 1992, Citicorp Credit Services, Inc., a subsidiary of Citicorp, agreed to settle charges that it aided and abetted a merchant engaged in unfair and deceptive activities. *Citicorp Credit Services, Inc.,* 116 F.T.C. 87 (1993). In 1993, the Shawmut Mortgage Company, an affiliate of Shawmut Bank Connecticut, N.A., and Shawmut Bank, agreed to pay almost one million dollars in consumer redress to settle allegations that it had discriminated based on race and national origin in mortgage lending. *United States v. Shawmut Mortgage Co.,* 3:93CV-2453AVC (D. Conn. Dec. 13, 1993). The Commission brought the *Shawmut* case jointly with the United States Department of Justice. In 1996, the J.C. Penney Company entered into a consent decree and paid a civil penalty to resolve allegations that the company failed to provide required notices of adverse actions to credit applicants. *United States v. J.C. Penney Co.,* CV964696 (E.D.N.Y. Oct. 8, 1996). In 1998, in conjunction with the law enforcement efforts of several state attorneys general, the Commission finalized a settlement agreement with Sears, Roebuck and Company that safeguards at least $100 million in consumer redress based on allegations that the company engaged in unfair and deceptive practices in its collection of credit card debts after the filing of consumer bankruptcy. *Sears, Roebuck and Co.,* C-3786, 1998 FTC LEXIS 21 (Feb. 27, 1998). The Commission also worked with state attorneys general in resolving allegations against other companies that involved practices in the collection of credit card debts after the debtors had filed for bankruptcy. *Montgomery Ward Corp.,* C-3839 (Dec. 11, 1998); *May Department Stores Co.,* File No. 972-3189, 1998 FTC LEXIS 117 (Nov. 2, 1998).

[17] Commission staff participates in numerous task forces and groups concerned with, for example, fair lending, leasing, subprime lending, electronic commerce, and fraud on the Internet, all of which have an impact on the financial services industry.

credit industry, and consumer and privacy advocates discussed the impact of identity theft on industry and on consumer victims. Subsequent press coverage helped to educate the public about the growth of consumer identity theft and the problems it creates. In November 1996, industry and consumer representatives reconvened in working groups to explore solutions and ways to bolster efforts to combat identity theft.

Having thereby developed a substantial base of knowledge about identity theft, the Commission testified before the Senate Judiciary Committee in May 1998 in support of the Identity Theft and Assumption Deterrence Act.

## III. THE IDENTITY THEFT AND ASSUMPTION DETERRENCE ACT OF 1998

Last fall, Congress passed the Identity Theft and Assumption Deterrence Act of 1998 ("Identity Theft Act" or "Act").[18] The Act addresses identity theft in two significant ways. First, the Act strengthens the criminal laws governing identity theft. Specifically, the Act amends 18 U.S.C. § 1028 ("Fraud and related activity in connection with identification documents") to make it a federal crime to:

> knowingly transfer[] or use[], without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.[19]

Previously, 18 U.S.C. § 1028 addressed only the fraudulent creation, use, or transfer of identification documents, and not theft or criminal use of the underlying personal information. Thus, the Act criminalizes fraud in connection with unlawful theft and misuse of personal identifying information itself, regardless of whether it appears or is used in documents. Furthermore, one who violates this prohibition and thereby obtains anything of value aggregating to $1000 or more during any one-year period, is subject to a fine and imprisonment of up 15 years.[20] These criminal provisions of the Act are enforced by the U.S. Department of Justice, working with investigatory agencies including the U.S. Secret Service, the Federal Bureau of Investigation, and the U.S. Postal Inspection Service.

The second way in which the Act addresses the problem of identity theft is by improving assistance to victims.[21] In particular, the Act provides for a centralized complaint and consumer education service for victims of identity theft, and gives the responsibility of developing this service to the Federal Trade Commission. The Act directs that the Commission establish procedures to: (1) log the receipt of complaints by victims of identity theft; (2) provide identity theft victims with informational materials; and (3) refer complaints to appropriate entities, including the major national consumer reporting agencies and law enforcement agencies.[22]

## IV. CURRENT EFFORTS: THE FTC'S CONSUMER ASSISTANCE PROGRAM

In enacting the Identity Theft Act, Congress recognized that coordinated efforts in this area are essential to best serve identity theft victims. Accordingly, the FTC's role under the Act is primarily one of managing information sharing among public and private entities in support of criminal law enforcement efforts,[23] and aiding vic-

---

[18] Pub. L. No. 105-318, 112 Stat. 3007 (1998).

[19] 18 U.S.C. § 1028(a)(7). The statute further defines "means of identification" to include "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual," including, among other things, name, address, social security number, driver's license number, biometric data, access devices (*i.e.*, credit cards), electronic identification number or routing code, and telecommunication identifying information.

[20] If the $1000 threshold is not met, the maximum penalty is three years imprisonment. The maximum penalty is increased to 20 years imprisonment if the identity theft offense is committed to facilitate a drug trafficking crime or in connection with a crime of violence, and 25 years if the offense is committed to facilitate an act of international terrorism.

[21] Because individual consumers' financial liability is often limited, prior to the passage of the Act, financial institutions, rather than individuals, tended to be viewed as the primary victims of identity theft. Setting up an assistance process for consumer victims is consistent with one of the Act's stated goals, to recognize the individual victims of identity theft. *See* S. Rep. No. 105-274, at 4 (1998).

[22] Pub. L. No. 105-318 § 5, 112 Stat. 3010 (1998).

[23] Most identity theft cases are best addressed through criminal prosecution. The FTC itself has no direct criminal law enforcement authority. Under its civil law enforcement authority provided by section 5 of the FTC Act, the Commission may, in appropriate cases, bring actions to stop practices that involve or facilitate identity theft. The practices the Commission expects to focus its law enforcement resources on are those where the effect is widespread and where civil remedies are likely to be effective. *See, e.g., FTC v. J.K. Publications, Inc., et al,* Docket No. CV 99-00044 ABC (AJWx) (C.D. Cal., filed January 5, 1999) (Alleging that defendants obtained

Continued

tims by serving as a central, Federal source of information. In order to fulfill the purposes of the Act, the Commission has developed and begun implementing a plan that centers on three principal components [24]:

(1) *Toll-free telephone line.* The Commission plans to establish a toll-free telephone number that consumers can call to report identity theft and to receive information and referrals to help them to resolve the problems that may have resulted. The identity theft toll-free number will build on the success of the Commission's two-year-old Consumer Response Center, a general purpose hotline for consumer information and complaints.

(2) *Identity theft complaint database.* The Commission is developing a database to track the identity theft complaints received by the FTC and other public and private entities. This database will allow the Commission to monitor better the extent and nature of identity theft. Moreover, the Commission expects that the database will enable the many agencies involved in combating identity theft to share and manage data so as to more effectively track down identity thieves and assist consumers.[25] For example, criminal law enforcement agencies could take advantage of a central repository of complaints to spot patterns that might not otherwise be apparent from isolated reports. In addition, a consumer with a concern that his or her social security number has been misused would not—and should not—need to call all the many federal agencies that could possibly be involved to ensure that the complaint was directed to the appropriate people. Under the planned system, the consumer could make a single phone call to one central number (the FTC's or that of any other agency sharing data with the Commission), to report the offense, have it referred to the appropriate agency, and receive additional information and assistance.

(3) *Consumer Education Materials.* A number of public and private organizations have published or begun developing materials that provide information on particular aspects of identity theft. The FTC is coordinating with others, both within and outside the government, to develop unified, comprehensive consumer education materials for victims of identity theft, and those concerned with preventing identity theft, and to make this information widely available.

Commission staff has been working hard to implement these plans. Phone counselors in our Consumer Response Center have been trained to handle identity theft complaints, and our general complaint database has been modified so as to permit entry of at least basic information about the identity theft complaints we already receive. In addition, we have recently issued a Consumer Alert that provides an overview of the steps consumers should take if they become victims of identity theft. We are also working with other government agencies to launch a web page in the near future devoted to identity theft information. The web page, which will include links to information from a number of government agencies, will be located on www.consumer.gov, the federal government's central site for consumer information.[26]

The Commission, in fact, has been working closely with other agencies in a number of ways in our effort to help consumers. For example, FTC staff has been working with the identity theft subcommittee of the Attorney General's Council on White Collar Crime to provide interim guidance to law enforcement field offices on how best to assist identity theft victims, and with the Social Security Administration's Inspector General to coordinate the handling of social security number misuse complaints. Most recently, Commission staff hosted a meeting on April 20, 1999, with representatives of approximately a dozen federal agencies as well as the National Association of Attorneys General. The meeting brought together individuals involved in diverse aspects of identity theft to discuss the implementation of the consumer assistance provisions of the Identity Theft Act. In particular, Commission staff

---

consumers' credit card numbers without their knowledge and billed consumers' accounts for unordered or fictitious Internet services).

[24] In the Identity Theft Act, Congress authorized the appropriation of such sums as may be necessary to carry out the FTC's obligations under the Act. Pub. L. No. 105-318 § 5(b), 112 Stat. 310 (1998). These plans are, of course, contingent on the actual appropriation of such funds. Should the volume of calls received from consumers approach the levels reported by Trans Union to the General Accounting Office, the appropriation required to respond to these calls may be substantial.

[25] The Commission has successfully undertaken a similar effort with respect to telemarketing fraud. The FTC's Consumer Sentinel network is a bi-national database of telemarketing, direct mail, and Internet complaints used by law enforcement officials throughout the U.S. and Canada.

[26] Www.consumer.gov is a multi-agency effort, with technical maintenance provided by the FTC. It contains a wide array of consumer information and currently has links to information from 61 federal agencies.

sought input from others in the design of the identity theft complaint database, to ensure that the FTC captures the information most useful to other agencies in both assisting consumers and catching identity thieves. In addition, this meeting was the first step in the FTC's efforts to develop a single set of consumer education materials. The Commission expects that a number of agencies will be working jointly with the Commission on this project to ensure that consumers have the best information possible on preventing and recovering from identity theft.

V. PRETEXTING

Related to identity theft is a practice known in the information broker industry as "pretexting." Pretexting involves obtaining confidential consumer information under false pretenses, *e.g.,* by lying and pretending to be the consumer. This tactic appears to be gaining popularity in response to the booming market for comprehensive personal information relating to consumers. Today, many information brokers tout their ability to obtain sensitive financial information—including current bank or brokerage account numbers and balances, which are not publicly available—without the subject ever knowing.[27] Pretexting is the method they use to obtain this information.

Pretexting may harm consumers in two related ways. First, there may be a significant invasion of the consumer's privacy resulting from the disclosure of private financial information through pretexting. Second, pretexting also may increase the risk of identity theft, resulting in serious economic harm. For example, using account balances and numbers obtained from a pretexter, an identity thief could deplete a bank account or liquidate a stock portfolio. The Commission just voted to file a complaint in federal district court against alleged pretexters. I will be prepared to discuss it at the hearing and the Commission will provide the Committee with a copy of its complaint and the concurring and dissenting statements of the Commissioners as soon as possible.

VI. CONCLUSION

Financial identity theft clearly continues to present a significant threat to consumers. The FTC looks forward to working with the Committee to find ways to prevent this crime and to assist its victims.

Mr. OXLEY. Thank you, Ms. Bernstein.

Mr. Albright.

## STATEMENT OF CHARLES A. ALBRIGHT

Mr. ALBRIGHT. Chairman Oxley, Chairman Tauzin, members of the committee, thank you for this opportunity to testify on behalf of the issue of identity theft.

My name is Charles Albright, and I am Chief Credit Officer of Household International. Household is a leading provider of consumer financial services and credit card products in the United States, Canada and the United Kingdom. I am here to offer a twofold perspective on this critical issue. First, from my personal experience as a victim of identity theft; and, second, from my professional experience at Household International in this area.

As you all know, identity theft occurs when a perpetrator gains access to another person's information and uses this information to commit financial fraud. Unfortunately, it is extremely easy to get access to some of this information in the marketplace today. This can be done by stealing someone's mail, going through their trash or even perpetration of employees at credit operation throughout

[27] *Id.* At last summer's hearings before the House Banking and Financial Services Committee, former and current information brokers described the recent explosion in the number—from a handful to hundreds—of information brokers offering confidential financial information, and noted that there are currently hundreds of Web pages available on the Internet advertising the ability of information brokers to obtain such information. *See Obtaining Confidential Financial Information by Pretexting: Hearings Before the House Comm. on Banking and Financial Services,* 105th Cong. (1998) (statements of Al Schweitzer, Robert Douglas).

the country. As an aside, it is not at all uncommon for a family member to commit identity theft upon another family member. In our experience at Household, we find that 50 percent of all incidences of identity theft are committed by another family member.

Armed with this information, the perpetrator will then open new accounts in the victim's name and access the victim's existing accounts. After running up significant debts, the perpetrator will likely fail to pay the charges, and ultimately the delinquency or bad debts will be reported on victim's credit report.

This is essentially what happened to me several years ago when, unbeknownst to me, someone obtained my personal information, including my Social Security number, and then proceeded to open several credit card and retail credit accounts in my name. The perpetrator had my address changed to a location in Philadelphia. For these accounts I received no statements or other information about the accounts. After opening these fraudulent accounts, the perpetrator proceeded to incur debts in tens of thousands of dollars. Believe me, I am very sympathetic with Mr. Anderson's comments today.

I would like to say, even though I have been in the consumer credit business for over 30 years, I intentionally worked through the entire process of trying to correct my personal situation myself; and I did not let anyone know in the credit reporting industry or even in the companies where I knew the senior executives that were carrying the balances on my accounts that this had happened. So I approached this strictly as a consumer, someone who reads USA Today and someone who hears about these stories.

I was unaware of any of this activity until 1 day when my wife received a telephone call at home from a collection agency after the debts had been delinquent for 60 days. It was at this time that I realized the scope of problem and began the lengthy and painstaking process of repairing my credit record. I spent countless hours dealing with credit grantors and credit bureaus sorting out this problem. I would like to state that in my case there was particular difficulty due to lack of response from two specific credit grantors.

While I was ultimately able to successfully resolve the situation after 18 months, I am nonetheless keenly aware of the problems related to identity theft and the difficulty in combating them. I believe it is fair to state that, since my experience, both the credit bureaus and creditors have become more sensitized and effective in dealing with this problem.

Household takes the issue of identity theft very seriously. We understand that dealing with the issue requires us to delicately balance the needs of our customers' expectations for expeditious credit decisions and efficiencies in granting credit, while taking prudent steps to adequately deal with the issues of fraud and identity theft as well as credit quality. Toward that end, Household has a team of over 200 dedicated professionals throughout the company who deal exclusively with the issues of consumer fraud. All employees undergo a thorough background check, including fingerprinting and criminal record investigations, to ensure that internal fraud is not perpetrated; and, unfortunately, this is not always the case. Sometimes, this does happen.

In addition, Household offers extensive employee training in this area, with an emphasis on customer service and counseling for those Household customers who have been victimized for true-name fraud.

In 1998, Household had more than 18,000 incidences of true-name fraud, with claims in excess of $35 million. The average size of an identity fraud case is approximately $1,600 to $2,000, depending on the business unit involved. It is important to note that the losses incurred are borne by the credit granting community, and in our case these losses go largely uncollected. In 30 percent of the cases, the customers either do not follow through on their claims of identity fraud or are found to have filed false claims.

When Household is contacted by a consumer who believes that they have been a victim of true-name fraud, we go through a series of steps to inform consumers of their rights and to assist in their efforts to rectify the situation. Household operates under the assumption that our customers have the benefit of the doubt in cases of identity theft and other types of fraud.

Once we have determined that there is a credible claim, we immediately put the customer's account in dispute, which means that the customer will not receive any calls from our collection department or that the account will be reported to the various credit bureaus as in dispute. This suppresses all balance and status information of the account to protect the consumer. From that point, we work with the consumer to complete the necessary affidavits and gather other documentation to assist in our efforts to process the claim.

Household dedicates a tremendous amount of resources to prevent such fraud from occurring throughout the entire credit granting process. We utilize sophisticated fraud modeling as well as a series of other steps to root out fraud and identity theft from the system. While credit grantors will never fully be able to stop instances of identity theft from occurring, we are making great progress in deterring such fraud through state-of-the-art technology and other prevention programs.

One problem we see in the credit granting community is that identity theft crimes are rarely prosecuted. Household also advocates that greater criminal penalties be placed on those who perpetrate such crimes, and we applaud those States that have recently acted in this area. Household also applauds Congress for enacting the Identity Theft and Assumption Deterrence Act of 1998, as it goes to the heart of the problem in dealing with combating identity theft.

Other problems in addressing this problem are that a number of different enforcement authorities have some jurisdictional problem and that identity fraud can surface in an array of financial crimes. Household concurs with the findings of the General Accounting Office in its report of May, 1998, detailing the jurisdictional challenges facing law enforcement entities as well as the limited statistics that exist in identifying the scope of this issue.

In closing, Household is committed to addressing this critical issue and has dedicated significant resources to combat this problem. I, for one, realize the devastating effect identity theft can have on an individual, having personally experienced it. Working to-

gether with Congress, I am confident we can shed light on this difficult problem and implement strategies to deter criminals from perpetrating fraud on honest individuals.

Thank you for the opportunity to testify today. I will be happy to answer any questions you may have.

[The prepared statement of Charles A. Albright follows:]

PREPARED STATEMENT OF CHARLES A. ALBRIGHT, CHIEF CREDIT OFFICER, HOUSEHOLD INTERNATIONAL, INC.

Chairman Oxley, Chairman Tauzin, members of the Subcommittees on Telecommunications, Trade & Consumer Protection, and Finance & Hazardous Materials, thank you for the opportunity to testify on the issue of identity theft. My name is Charles A. Albright and I am the Chief Credit Officer for Household International, Inc.[1] Household is a leading provider of consumer financial services and credit card products in the United States, Canada and the United Kingdom. I am here to offer a two-fold perspective on this critical issue, first from my personal experience as a victim of identity theft and the second from my professional experience at Household International, Inc. in this area.

As you all know, identity theft occurs when a perpetrator gains access to another person's information and uses this information to commit financial fraud. I would note that it is extremely easy for someone who seeks to commit fraud to obtain a person's private financial information. This can be done by stealing someone's mail, or going through their trash to find such information. As an aside, it is not at all uncommon for a family member to commit identity theft upon another family member, and in Household's experience, we find that 50% of all incidences of identify theft are committed by another family member.

Armed with this information, the perpetrator will then open up new accounts in the victim's name or access the victim's existing accounts. After running up significant debts, the perpetrator will likely fail to pay the charges, and ultimately the delinquency or bad debts will be reported on the victim's credit report. This is essentially what happened to me several years ago when, unbeknownst to me, someone fraudulently obtained my personal information, including my social security number, and then proceeded to open several credit card and retail credit accounts in my name. The perpetrator had my address changed to a location in Philadelphia, PA for these accounts so I received no statements or other information about the accounts. After opening these fraudulent accounts, the perpetrator proceeded to incur debts in the tens of thousands of dollars.

I was unaware of any of this activity until one day my wife received a telephone call at home from a collection agency after the debts had been delinquent for sixty days. It was at this time that I realized the scope of the problem and began the lengthy and painstaking process of repairing my credit record. I spent countless hours dealing with credit grantors and credit bureau agencies sorting out this problem. I would like to state that in my case there was particular difficulty due to the lack of response from two specific credit grantors. While I ultimately was able to successfully resolve this situation after many months, I am nonetheless keenly aware of the problems related with identity theft and the difficulty in combating them. I believe it is fair to state that since my experience, both the credit bureaus and creditors have become more sensitized and effective in dealing with this problem.

Household takes the issue of identity theft very seriously. We understand that dealing with the issue requires us to delicately balance the needs of our consumers' expectation for expeditious decisions and efficiencies in granting credit, while taking prudent steps to adequately deal with the issues of fraud and identity theft as well as credit quality. Toward that end, Household has a team of over 200 dedicated pro-

[1] Household International, Inc., headquartered in Illinois with major facilities in California, Nevada, New Jersey, Delaware, Florida, and Virginia, is a leading provider of consumer financial services and credit card products in the United States, Canada and the United Kingdom. Household has total assets in excess of $63 billion, employs over 25,000 people and provides financial services to more than 40 million customers. Household Finance Corporation (HFC), which recently completed its acquisition of Beneficial Corporation, is one of the oldest providers of consumer financial services in the United States, having been founded in 1878. Household's consumer finance business operates under the HFC and Beneficial brands, two of the oldest and best-known names in the consumer finance industry. HFC and Beneficial have over 1400 retail offices in 46 states as well as Canada and the United Kingdom. Household Credit Services and Household Retail Services are two of the nation's largest issuers of general purpose and private-label credit cards, including the GM Card and the AFL-CIO's Union Privilege card.

fessionals throughout the company who deal exclusively with issues of fraud. All employees undergo thorough background checks to ensure that internal fraud is not perpetrated. In addition, Household offers extensive employee training in this area, with an emphasis on customer service and counseling for those Household customers who have been victimized by true-name fraud.

In 1998, Household had more than 18,000 incidences of true-name fraud with claims in excess of $35 million. The average size of an identity fraud case is approximately $2000 for our consumer finance and retail services businesses and $1600 for our bank card business. It is important to note that the losses incurred are borne by the credit granting community, and in our case these losses go largely uncollected. In 30% of cases, customers either do not follow through on their claims of identity fraud or are found to have filed false claims.

When Household is contacted by a consumer who believes that they have been a victim of true-name fraud, we go through a series of steps designed to inform consumers of their rights and to assist in their efforts to rectify the situation. Household operates under the assumption that our customers have the benefit of doubt in cases of identity theft and other types of fraud. Once we have determined that there is a credible claim, we immediately put the customer's account in dispute, which means that the customer will not receive any calls from our collection department and that the account will be reported to the various credit bureaus as in dispute. This suppresses balance and status information of the account to protect the consumer. From that point, we work with the consumer to complete the necessary affidavits and gather other documentation to assist in our efforts to process the claim.

Household dedicates a tremendous amount of resources to prevent such fraud from occurring throughout the entire credit granting process. We utilize sophisticated fraud modeling, as well as a series of other steps to root out fraud and identity theft from the system. While credit grantors will never fully be able to stop instances of identity theft from occurring, we are making great progress in deterring such fraud through state of the art technology and other prevention programs. One problem we see in the credit granting community is that identity theft crimes are rarely prosecuted. Household also advocates that greater criminal penalties be placed on those who perpetrate such crimes, and we applaud those states who have recently acted in this area. Household also applauds Congress for enacting the "Identity Theft and Assumption Deterrence Act of 1998," as it goes to the heart of the problems in dealing with, and combating identity theft. Other difficulties in addressing this problem are that a number of different enforcement authorities have some jurisdiction over the problem and that identity fraud can surface in an array of financial crimes. Household concurs with the findings of the General Accounting Office in its report of May, 1998 detailing the jurisdictional challenges facing law enforcement entities as well the limited statistics that exist in identifying the scope of this issue.[2]

In closing, Household is committed to addressing this critical issue and has dedicated significant resources to combat this problem. I, for one, realize the devastating effect identity theft can have on an individual, having personally experienced such an ordeal. Working together with the Congress, I am confident we can shed light on this difficult problem and implement strategies to deter criminals from perpetrating fraud on honest individuals. Thank you for the opportunity to testify today. I would be happy to answer any questions you may have.

Mr. OXLEY. Thank you.

Mr. Connelly.

## STATEMENT OF D. BARRY CONNELLY

Mr. CONNELLY. My name is Barry Connelly, and I am the President of Associated Credit Bureaus. ACB is the international trade association representing over 600 consumer credit and mortgage reporting companies operating here in the United States and internationally.

We commend you for choosing to hold this oversight hearing on the crime of identity theft. Identity theft is an equal opportunity crime that affects everyone represented at this witness table. It is

[2] "Identity Fraud: Information on Prevalence, Cost, and Internet Impact is Limited," United States General Accounting Office, May, 1998.

a particularly invasive form of fraud where consumers, consumer reporting agencies and creditors must untangle the snarl of fraudulent accounts and information resulting from a criminal's actions. This task is often frustrating and time-consuming for all concerned.

I would like to join the others in acknowledging Congressman Shadegg's assistance and leadership in passing the Identity Theft and Assumption Deterrence Act. We think that the crime bill is a clear victory for all U.S. citizens.

Mr. Chairman, it is appropriate for me to depart from my prepared text and express to Mr. Anderson, on behalf of our association, my sincere regret for the difficulty that you have experienced. Naturally, I hope that it is the exception rather than the rule, and I don't have all of the facts from the companies you dealt with, but I would promise you, sir, I will do whatever I can to assist you in clarifying your situation, and I am sorry that it happened.

Mr. Chairman, consumer reporting agencies maintain information on individual consumer payment patterns associated with various types of credit obligations. The data compiled by these agencies is used by creditors and other as permitted under the strict rules of Fair Credit Reporting Act.

Consumer credit histories are derived from the voluntary provision of information about consumer payments on various types of credit accounts or other debts from thousands of data furnishers such as credit grantors, student loan accounts, child support enforcement agencies; and, in some cases, public record items do appear such as bankruptcy judgments and liens.

For purposes of data accuracy and proper identification, generally our members maintain information such as full name, current and previous addresses, Social Security number, and places of employment. This data is put into the system on a regular basis to ensure the completeness and accuracy of the data.

As important as knowing what we have in our files, it is also important to know what types of information our members do not maintain in their files. Our members do not know what consumers have purchased, and they do not know where they used a particular bank account card. They also don't have a record of when consumers have been declined credit or another benefit on the use of a consumer report. Medical treatment data is not a part of the consumer credit file.

Enacted in 1970, the Fair Credit Reporting Act was significantly amended in the 104th Congress with the passage of the Credit Reporting Reform Act. The Fair Credit Reporting Act serves as an example of successfully balancing the rights of the individual with the economic benefits of maintaining a competitive consumer reporting system so necessary to a market-oriented economy.

The Fair Credit Reporting Act protects the consumer by narrowly limiting the appropriate uses of a consumer report. Some of the more common uses of a consumer's file are in the issuance of credit, subsequent account review and collection processess. Reports are also permitted to be used by child support enforcement agencies when establishing levels of support.

A question that we hear with some frequency relates to how data found in a consumer's credit report may be used other than for credit reporting. Let me first point out that any data defined as a

consumer report under the FCRA may not be used for any purpose other than for those outlined in section 604.

It is a fact that some of our members do use consumer identification information to develop other high-value information-based products. Some of our members also develop direct marketing lists in order to stay competitive in the information marketplace. Again, note that the data used for direct marketing purposes is not the credit history information defined as a consumer report under the FCRA.

Identity theft is a crime that affects everyone. Our industry has a history of bringing forward initiatives to address fraud, and these efforts focus on use of new technologies and better procedures and education to reduce fraud. My written testimony lists a number of these initiatives, and I urge you to review them.

But in January, 1998, the ACB Board of Directors created a task force to insure our industry's focus on the issues of identity theft. The task force consists of the senior-most executives in our largest members.

The task force has progressed with a number of initiatives. Let me tell you that ACB has retained former Vermont Attorney General Jerry Diamond, who has an aggressive consumer protection record and who is former president of the National Association of Attorneys General. We hired him to act as an independent adviser to our industry on the specific issue of identity theft. Mr. Diamond's work helps our task force consider a broad range of concerns and ideas from external constituencies.

His work has included personal visits to each of the company fraud units. It has included interviews of the Secret Service, the Attorneys General and the FTC. He has talked with consumer advocates, he has interviewed victims of credit fraud crime, and he is opening up channels of communication with the National Association of Attorneys General.

In addition, the association created an Operations Working Group consisting of industry experts in fraud to explore the best practices and exchange ideas. We also formed a policy working group. This working groups seeks to keep the task force members informed on the types of issues and questions being raised by legislators and law enforcement.

The result of our work will be a series of initiatives and best practices which will focus on assisting victims to ensure that the consumer has a consistent experience in working with ACB members. It will attempt to be limiting the possible recurrence of identity theft, and it will develop and sponsor more consistent consumer information for victims and for crime prevention.

ACB and the FTC are currently exploring ways, as Mrs. Bernstein said, in which we can work cooperatively and effectively to implement the Identity Theft and Assumption Deterrence Act, but there are a few cautionary thoughts that I would like to leave with you.

It is difficult for laws to prescribe procedures and practices that prevent crime. Crime is a moving target, and, thus, our fraud prevention strategies must be as agile as the tactics of the criminals.

Information is a key economic growth factor in this country. Laws that limit information are most likely to merely take fraud

prevention tools out of the hands of legitimate industry. Ironically, to prevent fraud, we must be able to cross-check information. Absent this authentication of identifying information, we will be less able to prevent the very crime we are discussing here today.

Thank you for the opportunity to appear and answer questions.

[The prepared statement of D. Barry Connelly follows:]

PREPARED STATEMENT OF D. BARRY CONNELLY, PRESIDENT, ASSOCIATED CREDIT BUREAUS, INC.

Mr. Chairmen and members of the Subcommittees, my name is Barry Connelly and I am president of Associated Credit Bureaus, headquartered here in Washington, D.C. ACB, as we are commonly known, is the international trade association representing over 600 consumer credit and mortgage reporting companies operating here in the United States and around the world. Over 400 of our members are also in the collection service business.

We want to commend you for choosing to hold this oversight hearing on the crime of identity theft. Identity theft is an equal-opportunity crime that affects everyone represented at this witness table. It is a particularly invasive form of fraud where consumers, consumer reporting agencies and creditors must untangle the snarl of fraudulent accounts and information resulting from a criminal's actions. This task is often frustrating and time-consuming for all concerned.

Let me pause here to acknowledge that the leadership of one of your own committee members, Congressman John Shadegg, has helped us take an important step forward with regard to identity theft. His efforts resulted in the successful passage of the Identity Theft and Assumption Deterrence Act of 1998. This crime bill was a clear victory for every U.S. citizen, and our industry appreciates his attention to this important issue.

Before I discuss our concerns and industry efforts regarding identity theft, I have always found it helpful to first provide a short review of what a consumer reporting agency is, what is contained in a consumer report, and the law that governs our industry.

CONSUMER REPORTING AGENCIES AND CONSUMER REPORTS

Consumer reporting agencies maintain information on individual consumer payment patterns associated with various types of credit obligations.[1] The data compiled by these agencies is used by creditors and others permitted under the strict prescription of the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.) to review the consumer's file.

Consumer credit histories are derived from, among other sources, the voluntary provision of information about consumer payments on various types of credit accounts or other debts from thousands of data furnishers such as credit grantors, student loan guarantee and child support enforcement agencies. A consumer's file may also include public record items such as a bankruptcy filing, judgment or lien.

For purposes of data accuracy and proper identification, generally our members maintain information such as a consumer's full name, current and previous addresses, Social Security Number (when voluntarily provided by consumers) and places of employment. This data is loaded into the system on a regular basis to ensure the completeness and accuracy of data.[2]

It is interesting to note that the vast majority of data in our members' systems simply confirms what most of you would expect; that consumers pay their bills on time and are responsible, good credit risks. This contrasts with the majority of systems maintained in other countries, such as Japan or Italy, which store only negative data and do not give consumers recognition for the responsible management of their finances.

As important as knowing what we have in our files is also knowing what types of information our members *do not* maintain in files used to produce consumer reports. Our members do not know *what* consumers have purchased using credit (e.g.,

---

[1] Our members estimate that there are approximately 180 million credit active consumers. Since our members operate in competition with each other, these consumers are likely to have more than one credit history maintained.

[2] Note that there are in fact a number of major credit reporting systems in this country. Within ACB's membership the three most often recognized systems would be Equifax, Atlanta, GA; Experian, Orange, CA; and Trans Union, Chicago, IL. These systems not only manage their own data, but provide data processing services for the over 400 local independently-owned automated credit bureaus in the Association's membership.

a refrigerator, clothing, etc.) or *where* they used a particular bank card (e.g., which stores a consumer frequents). They also don't have a record of *when* consumers have been declined for credit or another benefit based on the use of a consumer report. Medical treatment data isn't a part of the databases and no bank account information is available in a consumer report.

THE FAIR CREDIT REPORTING ACT (FCRA)

In addition to our general discussion of the industry, we believe it is important for your Subcommittees to have a baseline understanding of the law which regulates our industry. Enacted in 1970, the Fair Credit Reporting Act was significantly amended in the 104th Congress with the passage of the Credit Reporting Reform Act.[3]

Congress, our Association's members, creditors and consumer groups spent over six years working through the modernization of what was the first privacy law enacted in this country (1970). This amendatory process resulted in a complete, current and forwarding-looking statute. The FCRA serves as an example of successfully balancing the rights of the individual with the economic benefits of maintaining a competitive consumer reporting system so necessary to a market-oriented economy.

The FCRA is an effective privacy statute, which protects the consumer by narrowly limiting the appropriate uses of a consumer report (often we call this a credit report) under Section 604 (15 U.S.C. 1681b), entitled "Permissible Purposes of Reports."

Some of the more common uses of a consumer's file are in the issuance of credit, subsequent account review and collection processes. Reports are also, for example, permitted to be used by child support enforcement agencies when establishing levels of support. A complete list of permissible purposes can be found under Appendix A of this testimony.

A question that we hear with some frequency relates to how data found in a consumer's credit report may be used other than for credit reporting. Let me first point out that any data defined as a "consumer report" under the FCRA may not be used for any purpose other than for those outlined under Section 604.

However it is a fact that some of our members do use consumer identification information to develop high-value information-based products such as fraud prevention and authentication products; risk management systems; and locator services, just to name a few. Some of our members also develop direct marketing lists in order to stay competitive in the information marketplace. Note that the data used for direct marketing purposes is not the credit history information defined as a "consumer report" under the FCRA.

Beyond protecting the privacy of the information contained in consumer reports, the FCRA also provides consumers with certain rights such as the right of access; the right to dispute any inaccurate information and have it corrected or removed; and the right to prosecute any person who accesses their information for an impermissible purpose. The law also includes a shared liability for data accuracy between consumer reporting agencies and furnishers of information to the system. Attached, as Appendix B is a text version of ACB's Brochure, "Credit Reports, Consumer Reporting Agencies and the Fair Credit Reporting Act—The Everything-You-Need-To-Know Guide to Consumer Rights in Consumer Credit Reporting".

IDENTITY THEFT

Let me now turn to the issue at hand—identity theft. As I said at the beginning, it is a crime that affects everyone. Our industry has a history of bringing forward initiatives to address fraud. These efforts focus on use of new technologies, and better procedures and education to reduce fraud.

Consider the following initiatives undertaken during this decade:

- ACB formed a Fraud and Security Task Force in 1993
- A "membership alert form" was developed to be used in notifying other ACB members of a customer, which was committing fraud through the misuse of data. Implemented in 1994.
- A "Universal Fraud Information Form" was developed for use by creditors when communicating the incidence of fraud to national consumer reporting systems.
- A generic credit reporting industry presentation on ACB fraud and security initiatives was developed and presented to customer segments during 1995.
- Minimum standards for data access equipment and software were announced to industry suppliers in March 1995.

[3] Public Law 104-208, Subtitle D, Chapter 1.

- ACB members implement company-specific limitations on the availability of account numbers, and truncation of Social Security Numbers on consumer reports sold to certain customer segments.
- Experian, Equifax and Trans Union voluntarily formed special fraud units with 800 number service and consumer relations personnel specially trained to work with fraud victims.
- A hardware and software certification program is created by the industry and administered by a third-party certification authority for those access products, which have implemented minimum industry security standards.
- Over 150,000 copies of a new customer educational brochure entitled "We Need Everyone's Help to Protect Consumer Privacy and Reduce Fraud" have been distributed since its first printing in the last Q.1997.
- An education program was also developed for use by ACB members in presenting the information found in the brochure. 2nd Q. 1998.

ACB TRUE NAME FRAUD TASK FORCE

In January of 1998, the ACB Board of Directors created a Task Force to ensure our industry's focus on the issues of identity theft. Its mission is to explore how our industry can continue to assist consumers and customers, which have been victimized by the crime of identity theft. The Task Force consists of the senior-most executives in our largest members.

Since its formation, the Task Force has progressed with a number of initiatives including:

(A) ACB has retained former Vermont Attorney General Jerry Diamond who has an aggressive consumer protection record, and who is a former president of the National Association of Attorneys General, to act as an independent advisor to our industry on the specific issue of identity theft. Diamond's work helps our Task Force consider a broad range of concerns and ideas from various external constituencies. Diamond's work has included:

1. Visits to the fraud units of the three national consumer reporting systems. These visits were opportunities for exploration of ideas and to learn from frontline operators, what consumers need and what challenges they face in assisting consumers.
2. Interviews with the Secret Service, Attorneys General, and the Federal Trade Commission.
3. Interviews with consumer advocates.
4. Interviews with victims of the crime.
5. Opening up channels of communication with the National Association of Attorneys General.

B. The Association created an Operations Working Group—the working group consists of industry experts in fraud to explore best practices, exchange ideas and ultimately to recommend a series of voluntary initiatives for our membership.

C. We also formed a Policy Working Group—this working group seeks to keep the Task Force members informed on the types of issues and questions being raised by legislators, regulators and law enforcement.

The results of our work will be a series of initiatives and best practices, which will focus on:

- Adopting best practices for assisting victims to ensure that the consumer has a consistent experience in working with ACB members.
- Adopting best practices for limiting the possible recurrence of identity fraud.
- Developing and sponsoring better and more consistent consumer information for victims and for crime prevention.

CONCLUSION

You can see on a number of fronts there is progress, and admittedly more to do.

We have better law, both in the states and at the federal level, which targets the crime and vigorous enforcement will be a key to effective deterrence. ACB and the FTC are currently exploring ways in which we can work cooperatively and effectively on fraud victim assistance. This dialogue is, in part, a positive result of the Identity Theft and Assumption Deterrence Act of 1998.

We have a very substantive industry-sponsored process going forward to develop initiatives that will be brought to completion later this year.

But there are a few cautionary thoughts that I would like to leave with each of you. It is difficult for laws to prescribe procedures and practices that prevent crime. Crime is a moving target and thus, our fraud prevention strategies must be as agile as the tactics of the criminals.

Information is a key economic growth factor in this country. Laws that limit information are most likely to merely take fraud prevention tools out of the hands of legitimate industry. Ironically, to prevent fraud you must be able to crosscheck information. Absent this authentication of identifying information, we will be less able to prevent the very crime we are discussing here today.

Thank you for this opportunity to testify.

Mr. TAUZIN. Thank you very much.

Mr. Oxley has gone to make the vote, and he will be returning to continue the hearing, and then I will leave to vote. Let me recognize myself for 5 minutes.

First of all, Mr. Anderson, I am a little confused. Did the Social Security Administration itself make an error in giving this man a Social Security card with your number on it or did he somehow participate in a fraud to get your number from the Social Security office?

Mr. ANDERSON. Well, because of the silence from Social Security, I have to go by the documentation that I have.

Mr. TAUZIN. Which is what?

Mr. ANDERSON. I have a letter which lists the offices, the person's name and their last given address in Cucamonga, California, as going into the offices in Glendora, Pomona, et cetera, California, and getting my number on five occasions.

Mr. TAUZIN. So the person, the perpetrator, went into the Social Security offices and got your number, but how did he get a card with your number on it?

Mr. ANDERSON. I don't know.

Mr. TAUZIN. Social Security has never explained that to you?

Mr. ANDERSON. They did not.

Mr. TAUZIN. But Social Security did issue him a card with your number on it?

Mr. ANDERSON. That is correct.

Mr. TAUZIN. Maybe Social Security has some answering to do here.

In your case, Mr. Albright, your Social Security number was obtained?

Mr. ALBRIGHT. I will tell you how I believe it was obtained. My resolution was never complete. I believe it was one of two major credit grantors where they had an internal employee which had access because I was a customer and had a credit relationship, where they had access to my personal financial information.

Mr. TAUZIN. In Virginia the Social Security number is your driver's license number. Every public official I know on this panel has filed documents with the SSN on it, either tax returns which have been made public or other documents under some sort of financial reporting requirements. Every student I know in most universities has the Social Security number as their ID number. I am told that some put it on tests. Every test has the Social Security number on it. I guess what I am saying is that it is pretty easy in our society to take your number and use it, isn't that correct?

Mr. ALBRIGHT. In this case, it was obviously an intent to create a crime.

Mr. TAUZIN. I am assuming that somebody has a bad intent. It is pretty easy to get the number?

Mr. ALBRIGHT. Yes. If I might finish, I would argue also the fact that that information is extremely valuable to a credit grantor to assist consumers.

Mr. TAUZIN. I accept that. I understand that.

But let's take it a step at a time. So somebody has got your number. In fact, Social Security gave him a card with your number which allowed him to use your credibility with a Social Security issued card with your number. So he goes out and he makes all of these charges and defrauds some companies out of money. And, as Mr. Shadegg said, you are not considered a victim because it was companies that were defrauded.

How about every customer in America who has to pay higher retail prices because the cost of business has increased? We have a lot of victims out there to deal with. You yourself, Mr. Anderson, finally, with Mr. Shadegg's legislation, is identified as a victim.

Knowing the number is fairly easy to obtain and knowing that there are people out there willing to do this, how do we protect people without compromising the availability of useful information? At the same time, how do we also make a lesson, an object lesson, of people who would do this?

Let me ask you, Mr. Anderson. You know the guy's name and address and where he lives in California. Have you ever been tempted to go out and egg his house?

Mr. ANDERSON. I have thought about it.

Mr. TAUZIN. Why haven't the enforcement authorities arrested the guy?

Mr. ANDERSON. We heard about that earlier. Basically, I started with the local law enforcement authorities in that county in California. They referred me to the Virginia State Police.

Mr. TAUZIN. You have been bounced around. Nobody has ever prosecuted this guy.

Mr. ANDERSON. I wound up after two trips to the FBI with Social Security. Only after intervention by Congressman Bliley a few months ago have I started to see any substantive action.

Mr. TAUZIN. I congratulate you on going to a good source. But does every member of our society have to know a congressman to get some help? Is that the only way you are going to get help?

Mr. ANDERSON. That is what it took.

Mr. TAUZIN. Isn't that awful? We have some work to do.

We have five reference points here. We have a perpetrator of fraud. We have a retailer, provider of goods and services. Neither one is going to be responsible for cleaning up this mess. The retailer is a victim. The perpetrator is the perpetrator. He is not going to clean it up.

You have three other people. You have the owner of the number, the owner of the credit who has been victimized. You have the credit reporting authority that now has a bad record and is reporting to other people about bad credit. And you have the issuer of the credit, the financier, the credit card.

I am going to have to run and go vote. Mr. Oxley will take over.

You have three points of reference now of responsibility. How much is the consumer responsible to clean up his own mess? How much is the finance company, the issuer of the credit card responsible for cleaning up the mess when the numbers that they have

issued have been used improperly to create bad credit and defraud people? And how much is a credit reporting agency, whose job it is to collect and send out good information to people that won't damage people and will help people, how much is it your responsibility to clean up this mess? And if we haven't figured it out, can we figure it out today?

Think about it. I am coming back.

Mr. Oxley.

Mr. OXLEY [presiding]. I will let Mr. Tauzin come back and finish up that line of questioning.

Let me ask you about the growth of identity theft, particularly Mr. Albright and Ms. Bernstein. It is obvious that identity theft is growing in recent years. In your experience, both of you, what are the causes? Why is there an explosion of this? Why is it happening now? What technology is available perhaps that wasn't available then?

Mr. Albright, let me begin with you.

Mr. ALBRIGHT. Thank you.

In our case, it has been rather explosive. I don't have the information in front of me going back in historical years. I know that it has increased exponentially for the last couple of years.

At our company last year we processed in excess of 30,000 claims of people who came to us and said that they were victims of credit card fraud or some type of identity fraud. Thirty percent of those people, when we sent out the appropriate forms and started asking the questions, we never heard from again, so that number now comes down to 70 percent. Of the 70 percent of the people left over, 80 percent were some type of identity fraud type situation. So that number just continues also to increase year after year after year.

Mr. OXLEY. Ms. Bernstein?

Ms. BERNSTEIN. Yes, thank you, Mr. Oxley.

We, too, have tried to gather some statistics on the extent of it; and the most recent data is from GAO that reports that consumer inquiries to the credit bureaus increased from 35,000 in 1992 to 522,000 in 1997, similar data from the Social Security Administration.

In response to why now, I think you alluded to some of the things that we are seeing happening. The techniques for perpetrating identity fraud used to be low-tech, getting information out of garbage cans or picking up a piece of mail with some identifier on it.

More recently, we have seen a more sophisticated technique in a practice known as skimming. Identity thieves use computers to read and store the information on a magnetic strip of an ATM or credit card. When that card is inserted either in a specialized card reader or legitimate payment mechanism and once it is stored, the information can be re-encoded on any other card with a magnetic strip, instantly transforming a blank card into an ATM or credit card identical to the victim.

There are undoubtedly technological mechanisms that have come into use now that are facilitating any thief who is engaged in those practices. So it has been, I believe, for a couple of reasons but because it is easier to do it in more ways.

Mr. OXLEY. So technology is our friend and our enemy?

Ms. BERNSTEIN. Exactly right. We are trying to stop it, so we are hopefully as smart as they are.

Mr. CONNELLY. Mr. Oxley, can I comment?

The 550,000 calls used in the GAO study came from one of my members, and it deserves some explanation because it is misleading.

That was the total number of calls that the fraud division of that company received in 1 year. In fact, the fraud division does not categorize them by specific categories, each call, such as a proactive call or questions about fraud, things like Mr. Albright described, people who call and maybe have lost their wallet and never had a fraud. I am not trying to minimize the seriousness of the number of instances but bring it into perspective, that it wasn't 550,000 theft fraud calls. Thank you for that opportunity.

Mr. OXLEY. Mr. Anderson, first of all, do you know whether the criminal who stole your identity has ever been prosecuted, to your knowledge?

Mr. ANDERSON. I have every reason to believe they have not.

Mr. OXLEY. When you had your discussion with the Special Agent in Charge from San Francisco, the FBI——

Mr. ANDERSON. Yes.

Mr. OXLEY. [continuing] Was it your understanding that the bureau had said that they didn't have the statutory authority to investigate identity theft at that time?

Mr. ANDERSON. No. It was my understanding that, with most law enforcement of that type, there seems to be a dollar threshold on what will or will not be accepted for prosecution and that—if I understood what the special agent was telling me correctly, he was telling me that my problem didn't rise to the level that the U.S. Attorney would take the case.

Mr. OXLEY. This was before Mr. Shadegg's bill became law; is that correct? Before the law was passed in the last Congress?

Mr. ANDERSON. Yes, it was. That was several years ago.

Mr. OXLEY. So it may have been that the only opportunity the Bureau had to investigate was under the major thefts statute; is that correct?

Mr. ANDERSON. That is correct. When the new law came out, since I was now dealing with Social Security Inspector General. I wrote to them and I said, here is a violation of 18 U.S. Code. What are you going to do about it?

Mr. OXLEY. But the initial statute that the Bureau had to act under was major theft, which does set a monetary amount, maybe $250,000. I can't remember now what the statute says, but that was the case.

Let me ask Ms. Bernstein, has any credit rating agency been found to have illegally sold or transferred data to another party?

Ms. BERNSTEIN. I'm sorry, I didn't understand your question.

Mr. OXLEY. Has any credit rating agency been found to have illegally sold or transferred data to another party?

Ms. BERNSTEIN. Not to my knowledge.

Mr. OXLEY. Within the scope of your jurisdiction, you don't know.

Mr. Connelly, do you know?

Mr. CONNELLY. No, not the way that the question is phrased.

Mr. OXLEY. What about any charges to that effect?

Mr. CONNELLY. Frankly, more to the contrary. There have been circumstances where an individual may have obtained information impermissibly from a consumer reporting agency.

Mr. OXLEY. Has any credit reporting agency ever violated the statute as it relates to providing data in your——

Mr. CONNELLY. Since 1971, since the law went into effect, there is certainly a body of case law in effect. Some consumers have succeeded in winning cases against consumer reporting agencies. Usually, it would be more a matter of the jury finding that the bureau exceeded the reasonable procedures and did make an error beyond the limit of reasonable procedures.

Mr. OXLEY. That is civil action?

Mr. CONNELLY. Those are civil actions, yes. I, frankly, don't know of any criminal actions. Again, the FTC, of course, in enforcing has brought some consent decrees, but again I don't know of any criminal situations where a consumer reporting agency has violated.

Ms. BERNSTEIN. The FTC's authority is all civil, and we have brought many enforcement cases over the years to enforce the provisions of the FCRA.

Mr. OXLEY. Many credit thieves send in a change of address to creditors to avoid detection for a longer period of time. Is there any way, working with the Postal Service, that credit bureaus can cross-check or send a notice to the old address when a new address is received and the credit history is updated? Mr. Connelly, is that something that we could——

Mr. CONNELLY. That certainly is something that our members would want to have access to be able to do.

Usually, I think Mr. Albright will speak to that, when they get a new address from consumers, they have methodologies at the credit grantors' point of information where they will attempt to reverify, and I don't think you will send a credit card to a new address without reverifying it. We get our address from the credit grantor who has submitted the data to us or from a consumer.

Mr. OXLEY. Mr. Albright?

Mr. ALBRIGHT. If I might just take a moment to explain, my situation was pretty straightforward, I believe.

Someone penetrated my personal data. They then had a Pennsylvania driver's license issued in my name with a new address in Philadelphia, Pennsylvania. They then took that piece of information, went in to these various retail stores and opened up an account under the Philadelphia address. They would have also had my previous address in Arlington Heights, Illinois, and they would complete the application.

They go into the credit bureau data base, and the data base looks, we do not have Charlie Albright with this Social Security number at this address, but we have him at the previous address in Chicago. They would presume Charlie Albright has relocated.

And this was not a real estate mortgage. These were $1,000 transactions, not $10,000 transactions. They would presume that Charlie Albright relocated and go through whatever algorithm required, and the credit file would be clear, and probably in a matter of seconds the account number was issued and the account was approved.

So credit information was a resident in Arlington Heights, Illinois. New address, a very transient society, we all have a tendency to move around. No reason to think that I was a criminal. They thought I took a new position in Philadelphia, and the criminals were off and running.

Mr. OXLEY. Which makes the enforcement and tracking and all of that just more difficult.

Mr. ALBRIGHT. When you get to enforcement also, in our case, at the end of day you are dealing with tens of millions of dollars. On a case-by-case business situation in our business you are talking about 1,600 to 2,000 transactions, and you just have one company. These things are not all bunched together, so you are not going to pursue them legally. No. 1, no one is going to listen to you, and, No. 2, the economics would not warrant it.

Mr. OXLEY. What about a situation where someone got your Social Security number, Mr. Anderson? That is how the whole thing started?

Mr. ANDERSON. That is right.

Mr. OXLEY. Shouldn't there be some ability of the Social Security Administration to check to see whether a particular Social Security number has already been obtained? In other words, had that individual applied for a SSN under your name, I would assume in Social Security they have the wherewithal to verify the fact that your name and your Social Security number are on file there so when somebody else went in to obtain that number it would come up that you already have a number and it is already matched with your name?

Mr. ANDERSON. Well, I would think so.

According to correspondence I have from Social Security, they have a process that they call reconciliation, and it is supposed to detect situations where a person is working under the same name and SSN. But, remember, before I started having the credit problems, I went face to face into a Social Security office in Baltimore, and they told me that they knew that there was a problem. The name that was on the document that they called me in was the same as mine with a different middle name, and it is the name of the alleged perpetrator that was given to me in the letter from Social Security.

So I think it is clear that they know who the person is, or they at least know an alias of the person. There is somebody there. I think they are well aware of that. They have a system in place called reconciliation. Why they didn't do something about this is a mystery to me, and it has only been in the last few months I have been able to get any momentum to push them at all. It has taken years.

Mr. OXLEY. Yes, Mr. Albright.

Mr. ALBRIGHT. It appears to me, in Mr. Anderson's case, you have a surgeon who has operated on a patient who used this information who clearly knows who this person is and where he lives. That doesn't happen very often.

Mr. OXLEY. So the middle name was different.

Mr. ANDERSON. That is what I understand, yes.

Mr. OXLEY. You don't know that for a fact?

Mr. ANDERSON. I just know what I have in documents, and the middle name has always been different until the medical visits that I told you about. The person was apparently hospitalized and went to two hospitals, and the hospitals, of course, called me with collections. After that, I had to verify who I was to the hospitals. I had to tell them my real middle name, and they asked me for my mother's maiden name and so on. After I provided that information to the hospitals to protect myself, this person started using better information. So somehow through the information I gave the hospitals in California, this person got additional information.

Mr. OXLEY. So we are talking about a pretty sophisticated individual?

Mr. ANDERSON. The person has been very selective. Every couple of months the person walks into a department store, rips them off and disappears. Until the medical business came, for whatever reason, there was not a really good trail. My letter to Social Security IG simply said, with medical records, I think it should be pretty simple to identify somebody, under the new law particularly. That is where I am with Social Security at this point.

Mr. OXLEY. Thank you.

The gentleman from Missouri, Mr. Blunt.

Mr. BLUNT. Thank you, Mr. Chairman; and thank you for having this hearing on implementation of the law that we passed last year.

We had a person in my district in southwest Missouri, Angela Williams, who really for 2 years was spending a substantial amount of her time just trying to restore her credit because of this very problem. And, of course, this as a civil matter was handled differently than I hope it will be in the future.

Mr. Anderson, what do you think could be done to help clean up the credit record more quickly once it has been determined that you are a victim?

Mr. ANDERSON. Well, I have thought about that. If this were a hockey game, I think I would like the credit reporting agencies to be the victims of a red light and a penalty box. When I go through all of the necessary procedures to notify both them and the provider of the information which I am disputing that I am a victim of bona fide Social Security fraud, that they go into the penalty box at that point and things stop and get corrected. That doesn't happen. It seems like we just shift into another round of the game. Maybe something gets corrected, maybe it doesn't. Maybe it gets partially corrected, and I am right back a month later writing the same letters, filing the same disputes and contacting the same providers of bad credit information.

Mr. BLUNT. Ms. Bernstein, there is a California law that was enacted last year that requires the credit reporting agencies to block reporting any information that the victim of identity theft alleges appeared improperly on their credit report as long as the victim submits a copy of a valid police report. Is that something that could be done nationwide and, if so, could you do it and what would we have to do?

Ms. BERNSTEIN. The FTC would have to be authorized, Congressman, in order to do that. There are already some efforts, and they would be more effective if they would be required by law to put a

fraud flag on the credit report as soon as Mr. Anderson's report was made, and that would in part do the same thing the California act is doing. Then nobody could rely on the information that has already been flagged in order to issue additional credit.

Mr. BLUNT. It would still be on the report?

Ms. BERNSTEIN. Yes. It would be on the report.

Mr. BLUNT. In the California case, they don't put the information out after the person has effectively filed the police report and done whatever else is necessary?

Ms. BERNSTEIN. That would seem to be—I am not familiar with the particular California law, but it would seem to be a very effective device.

Mr. BLUNT. Mr. Albright, from a credit officer's point of view, what are the problems with that? Do you have any information on how that is being implemented and what do you see as the problems? And what sort of responsibilities should the creditor have to stop sending out reports of debts incurred after they have been told that this is a person who is the victim of identity fraud?

Mr. ALBRIGHT. I am sure this has happened in our company, and I know everybody would be ashamed of it if we didn't respond, and let me tell you how our process works. Early on in the process, as I indicated in my opening testimony, I alluded to what I call a flag on the system. What that flag on the system does is it sends back a message electronically to a credit grantor that there is a fraud situation with this account. What we do in our company then is we force that account to be manually reviewed.

In that also there is a statement that says, I believe, to call the customer; there has been some fraudulent activity on this account. So in my case they would have called me or whatever.

Clearly, I believe that the creditor has a moral and business obligation when they are convinced that there has been an identity fraud situation to, No. 1, to put a flag on that account. I believe it has worked very, very well. Household has installed an automated process to make that go very quickly from us to the other credit grantors.

In addition to that, we remove the trade line entirely from the credit file. I believe the mechanics are there today.

My personal situation is that I was treated as a criminal by the credit grantors. One of my charges was at a store in Wilkes-Barre, Pennsylvania, for $1,800 for automobile repair. I don't own that type of car, and I was told on the telephone that I was lying and I made that type of repair. This is a very, very large organization, and they really got my attention when they called me a liar. I am a credit grantor but also a consumer. But, in any event, in my case no one believed that I was telling the truth. Even when you go through all of the documentation.

Finally, how I got it resolved is I knew the general counsel personally of the company that was involved. After 18 months I called him on the phone; and I said, look, I have a file here that is about 6 inches thick. I have return receipts and certified letters. I have not been harmed personally because I have not applied for credit. I know what my credit bureau file looks like. I said, I am ready to start litigation. What would happen if a senior credit executive were to sue your company for this performance?

He came back to me and he said, if you have what you say you have and you are right, we will write you a check today for $2 to $3 million to go away. This case is so ugly, we don't want this to go any ways. I indicated I wanted it fixed, and it was fixed by the time the sun went down that night.

What that tells you, the mechanics are in places—training, education, and sensitivity. Credit grantors have that obligation to employees. Make sure that we are hiring the right people.

At Household, we have internal employees in our bank card operation that have perpetrated fraud, where they have confiscated information from our card holders and done the same thing to innocent people that was done to me. If we catch them, we prosecute them, and we try to take them to the extreme extent of the law. A lot of laws are there today. It is a matter of people utilizing the system.

Mr. BLUNT. Mr. Connelly, I cosponsored Mr. Shadegg's bill last year. I understand why we needed to make this a crime. I know that it is a tough job, and you have lots of vulnerability out there with the information you give out being accurate. Why hasn't the industry solved this problem like the California law or other States are now trying to require it be solved? Why hasn't this been done?

The industry would have done this better than government would have if they would have done it, and I am asking you why they didn't do it and how far along you are on a national standard that accomplishes these kinds of things once you are convinced there was a legitimate problem.

Mr. CONNELLY. Thank you for asking that question, and in my prepared testimony I hope that I made clear to the committee that indeed Associated Credit Bureaus and our members do recognize it as a problem, and we are trying to do it individually or without government assistance other than things like making it a criminal activity.

Each of our companies, the three major companies, have dedicated fraud units to handle the cases like Mr. Anderson's. And I can't tell you what happened, where his went awry; and I commented on that before.

But, as Mr. Albright said, as soon as one of our companies is notified of a possible fraud, even the potentiality of a fraud, a call from a consumer, that file is flagged. So, if it didn't happen in Mr. Anderson's case, I can't give you the information why without going into the specifics. As a policy, that happens each time.

So you heard Mr. Albright explain that in his company they see the flag, they take the flag seriously on an application for credit. If a company, a credit grantor, does not take that flag seriously, the flag is worthless. It is like a red light that is out there, and someone goes through the red light, and that is going to perpetuate the crime. So a flag is not the only answer.

Mr. BLUNT. Is this such a big problem that you can't do more than just flag the file?

Mr. CONNELLY. That is one thing.

Let me speak to the California case that you just described.

Yes, in California if a consumer presents a police report, I am going to call it the individual trade line, the individual item that

is disputed as being a victim of fraud is deleted or blocked from the credit history. And that is fine. We would all agree with that.

The trouble is, let me tell you what is happening. What we are seeing now is an increased number of credit repair clinics, additional con artists who are using this legitimate tool as a tool to eliminate and strike from the file legitimate adverse credit history from other consumers. So then the Albrights of the world and the Households and the rest of the credit grantors get stuck for not being able to get true information on truly adverse paying customers.

So, yes, that is one thing. I am showing you another side to it that makes it not a perfect solution.

Mr. BLUNT. Thank you, Mr. Chairman.

Mr. TAUZIN [presiding]. The gentleman——

Mr. ALBRIGHT. I did not answer the last part of your comment about the California situation. I was told two things specifically as I queried all of our business units, knowing that I was going to be coming here.

No. 1, Charlie, be very careful about the California situation in terms of police reports because, in many jurisdictions, I have been told, it is not very complicated to get a police report, and it could perpetuate the crimes if the wrong people get onto that.

No. 2, try to get the message across that there needs attention to this whole situation of law enforcement agencies because, working with them today, we cannot get them to be interested, and that gets back to the heart of the discussion we have been talking back.

Mr. BLUNT. I would not mind to have Mr. Anderson's comment.

Mr. ANDERSON. I honestly believe in virtually every case of successful theft from department stores and hospitals, that had the people granting the credit done a positive ID, somehow positively identified the person that they were dealing with other than just asking for a Social Security number, there would not be a problem. I think that the creditors are lax in identifying and knowing who they are doing business with.

Ms. BERNSTEIN. That has been our experience as well. There has been really insufficient attention of credit grantors to whom they are granting credit and ignoring the flags that are on the credit bureau reports as well.

Mr. BLUNT. By ignoring the flags, do you mean that they don't understand the flags and they assume that this person is in trouble, or they just ignore the whole report?

Ms. BERNSTEIN. It is a mixed bag, I believe, to the best of our knowledge.

Mr. TAUZIN. The Chair is going to ask the agreement of Mr. Shadegg, and we will turn the time over to him in just a second. I am being called to the Appropriations Committee.

I just wanted to get an answer to the question that I posed. And the question is, among the three reference points, excluding government, which should be the enforcer in the end, but among the three reference points, the consumer, the credit bureau or reporting agency, and the person handling the financing, issuing the credit cards, extending the credit, among those three players, who has a responsibility for cleaning up the record and making sure that Mr. Anderson doesn't have to wait 5 years?

Let me pose it quickly maybe a different way.

If Mr. Anderson supplies your member company, Mr. Connelly, with information that he has been defrauded, is it your responsibility to make sure all of the companies get proper information that he is not, in fact, a bad credit risk? Is it your responsibility today and do you assume that responsibility? Does it need to be clarified in law or regulation?

Mr. Albright, in terms of the issue of the credit card, how much responsibility does the issuer of the credit card or the financing, the extension of credit, have in terms of helping Mr. Anderson clear up his record?

It is to your benefit to give him that credit card. I get them in the mail all the time unrequested. There must be some real value in having me as a credit card holder.

He has now been damaged. How much responsibility do you have to help insure that his records are cleared up? Somebody has some responsibility. He may have some to properly document the problem. I think he has taken 5 years to do it. You yourself, Mr. Albright, mentioned the time it took you.

But once you have documented, which one of you are most responsible or what do you share in responsibility in cleaning this up so he doesn't have to go to Mr. Bliley and say, Congressman, it doesn't work out there, and I need you to intercede with somebody. Which one of you is most responsible or how do you share that responsibility? Please respond.

Mr. ALBRIGHT. I believe Household in this case has a very clear responsibility once we start the investigation of fraud to, No. 1, flag the account as being under investigation. Again, there is no guilt or innocence here, because the case is not resolved, the fact that we have been contacted. We code the account, put the flag out there.

Mr. TAUZIN. Is it your responsibility to notify?

Mr. ALBRIGHT. It is my responsibility to notify him.

Mr. TAUZIN. It is your responsibility to notify him that his number has been compromised and it ain't his fault? He has done nothing wrong.

Mr. ALBRIGHT. He has notified me.

Mr. TAUZIN. Notified you timely. You have corrected the records. You may have taken a loss yourself in the process, but now your job is to notify Mr. Connelly's member. What is your member's responsibility?

Mr. CONNELLY. Our responsibility in the instant case you just described is to delete the information and not let it reappear on the file.

Mr. TAUZIN. Why has that not happened for Mr. Anderson? Does anybody know? Mr. Anderson, do you know why it hasn't happened?

Mr. ANDERSON. No, but I think somebody named Glen King does.

Mr. TAUZIN. Who is Glen King?

Mr. ANDERSON. The one that sends most of the letters ignoring what I am doing from Equifax.

Mr. TAUZIN. So Glen King is a guy in this credit reporting agency?

Mr. ANDERSON. For years.

Mr. TAUZIN. So you have a problem with one of your members. Is that credit agency a member of your association?

Mr. CONNELLY. Yes, they are, sir.

Mr. TAUZIN. Do you have self-policing structures within your organization?

Mr. CONNELLY. The Fair Credit Reporting Act, as amended, speaks very strongly to that. We do not have Mr. King's side of the story.

I think you will allow me to just make the point that what occurs in the instance that we just discussed, Mr. Albright received the example of a fraud notice at his company. Mr. Albright, who is a regular contributor of data to us, notifies us that that information is wrong, and it is not to be reported again. We have to stop reporting it, absolutely.

Mr. TAUZIN. What is wrong with this guy King?

Mr. CONNELLY. There are other circumstances.

Mr. TAUZIN. What are the other circumstances?

Mr. CONNELLY. Maybe Mr. Anderson came directly to the consumer reporting agency and said, the item on your report from Household, we will use you as an example, is a fraud account. In this case, the consumer reporting agency member of ours, under the laws of the Fair Credit Reporting Act, is required within 30 days to go back to the credit grantor and reverify the information. If they cannot reverify it, it must be deleted.

I am going to make an assumption here that Mr. King is getting back a reverified piece of data from whoever he is going to, and, therefore, he keeps reporting the data based on the reverification from the furnisher of the data.

Mr. TAUZIN. So what you are saying, in Mr. Anderson's case, the credit supplier is still reporting to the credit bureau——

Mr. CONNELLY. Yes, sir.

Mr. TAUZIN. [continuing] that Mr. Anderson is a bad guy and not paying his bills?

Mr. CONNELLY. They are reconfirming the data that the credit bureau has.

Mr. TAUZIN. Mr. Albright, it sounds like your guys are not doing their job here. Is that the case?

Mr. ALBRIGHT. If my guys are the credit grantors, it sounds like that to me, yes, they are not. I picked up a comment very early in Mr. Anderson's testimony that he kept going back to the credit grantor, and they kept saying that they had the Social Security number, and there wasn't anything that they could do, and it was a legitimate Social Security number and whatever.

Mr. TAUZIN. Here is where we are going to leave it. I am going to turn it over to the guy who knows more about this than anyone on the committee, John Shadegg.

What I am pointing out is that a guy like Mr. Anderson just gets bounced around. Not only does he get bounced around by the three corners of this triangle but also by the enforcement agencies that don't necessarily take him seriously or prosecute people. So he is left with the frustration that says maybe I am going to go egg the guy's house, and now I have to file a lawsuit and go after that $2 million claim. Maybe I ought to be one of those special people who knows his congressman well enough to get him excited, like Mr.

Bliley. Are we going to leave it like this, where everybody in America has to know somebody in Washington to get some help?

Mr. Shadegg, take it.

Mr. SHADEGG. Thank you, Mr. Chairman. I think we had a great illustration of the exact problem that exists and the frustration that occurs. I appreciate your efforts, Mr. Chairman. It really is true.

I think what we just described is that Mr. Anderson calls and says, I am not the guy that did the bad thing, but the creditor does not necessarily accept his word. There is a dispute, and the credit bureau continues to hear from the creditor that this person with this name and Social Security number is the bad credit risk, and Mr. Anderson keeps fighting the fight.

Mr. Anderson, let me start with you. Your statement was eloquent in making the points that need to be made; and it might even suggest, Mr. Chairman, that we ought to go to a new system. On the front of Mr. Anderson's statement he puts a little synopsis that says major points. You did a marvelous job of putting forth the major points, and our normal witnesses don't do that. I want to pick a couple of those points.

One point that I discovered is very true. It may have been more true when you incurred this problem. You say, very little assistance forthcoming from Federal agencies. I will tell you very little assistance is forthcoming for victims of this crime from either Federal agencies or State agencies. Because, even in the States where we have it, I have discovered through the task force that we set up this year in Arizona to try to make sure that the State law is being implemented and the Federal law which I got passed last year is being implemented, in point of fact, agencies are not providing assistance. I hope to get more heat on those agencies to provide assistance, because someone has got to get in there and solve the problem.

As an aside on that point, one thing I would like to offer to do is to work with you in trying to get Virginia, the State of Virginia, to pass a law like the State of Arizona did to deal with this problem. Because, in addition to having a Federal law, I think we need a State law. Because we need to bring to bear all of the law enforcement agencies that are possible.

The second point I want to make is you said you contacted the FBI and the Social Security Administration. Were there any other law enforcement agencies that you contacted to say, hey, I am the victim of a crime or I am being defrauded? Or were those the two that you principally worked through?

Mr. ANDERSON. Yes. In my review I started with the local authorities in California. I thought that was appropriate.

Mr. SHADEGG. State authorities?

Mr. ANDERSON. County, actually, because it was clear where this was happening.

Mr. SHADEGG. What was your experience?

Mr. ANDERSON. They referred me to the Virginia State Police. I talked to the Virginia State Police and explained to them what was going on; and they said, this is a Federal matter. You need to talk to the Feds.

So I looked at the choices with the Feds, and I found out, well, it wasn't postal fraud, not a credit card, so it is not Secret Service. The only thing I could come up with was that it might be Social Security, and it might be interstate telephone fraud, and that is why I contacted the agencies that I did.

But let me say this. I tend to be a stubborn person, and I can throw out a possibility here. If I had not done a thing, let us assume for a minute that I don't need credit, that I don't care about my credit report. If I had not done a thing in this case and I had not notified anybody, the only thing that would have happened is the department stores in California would be losing more money and the hospitals in California would be losing more money treating somebody that they don't know, that they don't even understand the identity of. That is what would have happened had I done nothing.

Mr. SHADEGG. I would argue that you are still a victim of the crime. Many people don't discover this until they pull a credit report.

When we introduced the bill last year, we held a press conference here in the Capitol; and many Capitol Hill staffers related that they had been victims of the crime. But one of the fascinating stories, a woman who lived in Northern Virginia, and I will tell the story, she said she went home 1 day and a friend of hers called her. The friend lived out of town and said, gee, I have been having a hard time getting ahold of you. I would like to see you when I am in town.

Why are you having a hard time getting ahold of me?

Your number is unlisted.

This woman said, no, my number is not unlisted.

And the woman said, yes, it is. I finally got it from a mutual friend of ours.

That afternoon the woman calls the phone company and said, is my phone unlisted?

They say, yes.

How did it get unlisted?

Well, your husband called and unlisted it.

So that night at the dinner table she turns to her husband, honey, why did you unlist our phone number?

He says, what do you mean? I didn't unlist our phone number.

What had happened was that the perpetrator of the crime who was going out in Northern Virginia and applying for credit did not want the credit issuers to be able to contact the real people, so the perpetrator of the crime had called the phone company and had their home phone number unlisted unbeknownst to them. The permutations of this crime are fascinating.

I guess the second point I want to make and that you make in your statement is that identity theft violations may not rise to the necessary dollar level to cause Federal law enforcement agency actions.

In the bill last year, we reduced the jurisdictional legal limit from $25,000 down to under $1,000 to enable them to deal with this problem; and I personally think your credit reputation is worth more than a thousand dollars, as is any American's. But the real

problem then becomes a resource problem, and that is something that I want to talk with the other gentlemen about.

But before I do, Mrs. Bernstein, I want to ask you just very quickly, the law that we passed last year gives you three specific functions, and I understand that you are working on all three of them and expect to meet the 1-year statutory deadline. My question is on funding. Has the FTC sought in the appropriation process the funding for these functions and are you receiving it?

Ms. BERNSTEIN. We have sought them. We have asked for $2.6 million over 3 years, which will provide us with probably not the maximum amount to take the maximum number of calls and carry out these duties, but we think it will allow us to be successful in carrying out the first phases of this program.

Mr. SHADEGG. Well, I guess the only point I would want to make is, if you are not successful or if you are having difficulty, please come and see me.

Ms. BERNSTEIN. I would not hesitate for a minute.

Mr. SHADEGG. I want to now turn my questions to Mr. Albright and Mr. Connelly.

Mr. Albright, in your testimony you, I think, hit the nail on the head, or at least one of the nails, in that you say one problem is that identity theft crimes are rarely prosecuted. We have just heard Mr. Anderson describe it. When you contacted the FBI, Mr. Anderson, and the Social Security Administration, that was before the effective date of last year's legislation? It was before last October?

Mr. ANDERSON. It was indeed. And the first letter that I wrote after I saw that change to the 18 U.S. Code was to the Inspector General of the Social Security Administration, and I asked point blank if they were going to enforce the criminal law.

Mr. SHADEGG. If you did not get their attention, in addition to perhaps using Mr. Bliley's office to get their attention, I would be happy to help.

Mr. Albright, the firsthand experience I had with this aspect of the problem was when we convened the task force; and I literally sat there with law enforcement agencies on one side of the room and prosecutors' offices on the other side and alphabet soup from FBI to FTC in the room. You saw everybody do this. We cannot prosecute this. This occurred in Virginia. The Virginia Police say this occurred in California. I think that is where we have to go to get to the heart of this problem, and I am not convinced that criminal law enforcement agencies are the answer.

You go on to say that greater criminal penalties should be placed on those who perpetrate such crimes. On the one hand, I see the criminal law as the proper method because a civil remedy may not be effectual because these people have no resources. So perhaps a criminal penalty is the right penalty.

But then the question is, how do we motivate law enforcement agencies to go after a criminal penalty where what you have is small dollar crimes like a $300 charge on a cell phone? The agency says look, we have $200,000 frauds to deal with. We can't devote any resources to go after this.

On the one hand, I see criminal penalties being appropriate. On the other hand, I see Mr. Anderson as the greatest victim and my

own constituents, Mr. and Mrs. Hartle, as the victims. It is clear that the people that you represent in this discussion, the creditors, are the direct victims; and the credit reporting agencies are becoming victims because people are becoming angrier and angrier at credit reporting agencies for their involvement.

Has any thought been given to something along the line of a RICO-type enforcement or something along the line of empowering creditors to collectively go after these people to stop their activity?

Or maybe even, turning to you, Mr. Connelly, maybe even a joint effort where the credit industry and the credit reporting industry go together and not just do the things that you talked about, Mr. Connelly, but actually fund efforts by the private sector to go after these people. Because while Mr. Anderson is the victim emotionally and his credit is destroyed, and I personally know what that means when you try to get credit and your credit is not in good shape, that can be a serious problem.

What is the remedy? I am asking both Mr. Albright and Mr. Connelly to comment on what other things can we do? Perhaps make it a RICO predicate or something in that nature, something that gives us the aggregate authority to go after these people?

Because while Mr. Anderson is in part the victim, and I worry about him, the money that is being lost is coming from you, Mr. Albright. And, quite frankly, I think it is ultimately coming from us because, to the degree that they defraud you, your stores, the people who you represent have to build into the prices of the goods I buy the cost of the goods to cover for the people who don't pay for the goods that they are stealing.

Do either one of you have a response to that?

Mr. ALBRIGHT. No. 1, in my particular case, I don't think it was ever discovered who to go after in the first place. I think that probably happens a larger percentage of time, is you really don't know because the statements in Philadelphia were going to an empty lot and everyone was, I am sure, long gone. The only thing I ever saw was a copy of the driver's license that was used and some of the documentation.

Mr. SHADEGG. Let me ask, isn't it possible if you were sufficiently on top of this and if a law enforcement agency was sufficiently on top of this, if someone walks in and applies for credit and they use a Social Security number or some other personally identifying information which you have already established has been used elsewhere to get fraudulent credit, could they be told, could you just wait here for a moment, and a law enforcement person could show up and arrest that person on the site?

Mr. ALBRIGHT. At times, that happens. Everything has to come together exactly.

Mr. SHADEGG. That would require greater awareness and effort by the credit-extending institution and the law enforcement agency.

Mr. ALBRIGHT. Years ago, when I worked in the retail environment for retail stores, where you have point of sale credit, which is really what we are dealing with here, I know even back in the 1970's and in the 1980's it was not unusual for us to call the Detroit Police Department or the Cleveland Police Department and ask them to go to such a location of a store and arrest a person.

Another issue comes to mind and anecdotal from what I hear, I believe the court systems are really overburdened, and there is tremendous case backlogs. That is one issue.

I think that, if possible, we are sort of getting into an area that I don't feel real comfortable telling you how to fix it. I don't know how to fix it. If I could discuss this with internal security people who deal with this all the time and send you back a letter with my thoughts, I would feel more comfortable, because I honestly don't know what the solution is. It is such a difficult issue to get our arms around.

I do know that our people have continuously told me, even if they have a situation, they can't get law enforcement's attention on it because of the size and the volume.

Mr. SHADEGG. Well, just to interrupt you for a moment, I certainly want to let you know I want to figure out how to get law enforcement's attention. Because it does no good to pass a law to help Mr. Anderson if law enforcement says they are penny-ante crimes and I am not going to do anything about it. I assure you, every victim feels it is a significant crime.

Mr. CONNELLY. Mr. Shadegg, I think I can safely say people like Mr. Albright, Household, and my members would entertain any ideas, like a RICO statute. I am not a good spokesperson on criminal prosecution, so I wouldn't want to go beyond that, other than to guarantee you that we would be open to entertain any suggestion like that.

I might, by example, show you another possible approach. It doesn't have the big hammer, but we were very frustrated after about 25 years, from 1971 until just recently, during the existence of the original Fair Credit Reporting Act, because there is a section in there that makes it an impermissible purpose for you to obtain my credit report fraudulently for a wrong purpose, and our members were getting hit with the reputation of letting anybody obtain the credit report of a consumer, which was not the case. We would go to local authorities to try to prosecute against the perpetrator who has obtained a copy of the report. The experience was the same. No enforcement.

When it came time to amend the Fair Credit Reporting Act that went into effect in 1997, the Federal Trade Commission supported us in this effort and everybody else did in making it a civil offense for you to obtain my report for an impermissible purpose. And, therefore, I can, as a consumer, sue you if you have anything to sue for, and also the consumer reporting agency can sue you for violating the Fair Credit Reporting Act.

There is a possibility that there is something to be said about Mr. Anderson having the ability to sue if he can find the person who perpetrated the crime and the credit grantors being able to bring a civil action against the consumer. I think you and I both know that the biggest deterrent here is the potential that that might happen. The potential that I might get sued for obtaining a consumer report for an impermissible purpose is more of a deterrent. It is a mild approach, but it is an approach.

Mr. SHADEGG. It is an interesting idea.

Let me ask the three of you not here in the role of victims, do all three of you agree that a part of this problem is caused by credi-

tors extending credit without sufficiently verifying the identity of individual?

Ms. Bernstein, do you agree with that?

Ms. BERNSTEIN. I do agree with that. I very much agree with that and think that more attention really should be paid to that aspect.

If I may add, in connection with your prior question, Mr. Shadegg, it has been our experience that the credit card companies have developed investigative capacity and have developed things like a profile so that the kinds of things Mr. Anderson was mentioning—two addresses, for example, for a person—would immediately get the attention before credit is granted.

So before I am too negative on credit grantors, which I don't intend to be, they have in some instances given us information so we can use it in our civil enforcement of the Fair Credit Reporting Act, such as where they have an early indication before we do that something is going on they notify us so we can investigate further.

Mr. SHADEGG. Do you agree that part of the problem is caused by creditors?

Mr. ALBRIGHT. Not totally. In my situation, it was a driver's license with a picture presented. There was an address. There was probably a Social Security card, pretty standard type of information to identify a real person there. All of the information was recorded on the application. So, you know, we were dealing with some relatively sophisticated people who knew how to get this information.

In our particular situation, we have multiple traps in the bank card operation which we are a pretty large player in, to try to catch certain red flags.

For example, if a consumer changes an address on the response coupon, that will be kicked out for someone to actually look at. If there is some type of a mismatch with the Social Security number, where a digit is off or the address is off by a digit, that is kicked off for a human type of intervention. At that point in time, Mr. Congressman, we don't open up the account until we talk with a customer and ascertain that we are dealing with the consumer.

Particularly in the bank card area, this is pretty sophisticated. Fraud is a very large item on all of our income statements. We are really trying to focus on making sure it is not eyeball to eyeball, and it never will be, but that we are dealing with who we think we are dealing with in the situation.

So I am sure there are some people out there who are lax, but for those credit grantors who are doing most of the business, they are really focused on trying to make sure that the right customer is being served.

Mr. SHADEGG. Mr. Connelly, do you think that it is part of the problem?

Mr. CONNELLY. I don't think that there is any credit grantor that is intentionally letting something occur in order to have a fraudulent account show up on their books.

I might say that, and I think Mr. Albright would agree with me, that the competitive atmosphere for issuing of credit cards has been such that perhaps it has invited or let in people who you might otherwise not have had as a victim.

Mr. SHADEGG. Mr. Anderson, do you think that is a part of the problem? Did you feel that those creditors in California who extended credit to this individual that is now using your name were too lax in extending credit to him or her?

Mr. ANDERSON. In the case of the department stores, I can certainly understand the need to do business and the competitiveness. They didn't know who they were doing business with in this case. In the case of the hospitals that performed surgery on the person, I think it is absurd. The whole litany of medical things that are on my report now, many are cleared up, I don't understand how you can perform medical services on somebody and not verify who the person is. The department stores, maybe not. I don't know.

Mr. SHADEGG. I am clearing exploring for a way to solve this problem. And it seems to me that, with some reservation, if, in fact, a part of the problem is that credit is extended too casually without taking sufficient steps to verify who the individual is, one remedy, which I am not saying that I would want necessarily to go to, would be to give Mr. Anderson a specific remedy and perhaps enhanced penalties to go after anybody involved in this from a negligence standpoint, the Social Security Administration, which should not have given out this card; or to go after a credit-issuing agency, Mervyns department store, for example, in your testimony, and give him a right to recover against them from the wrongful extension of credit to someone who wasn't him.

Commerce will say that is a terrible thing to have happen. But, by the same token, something has to be done to incent those involved in this to bring a halt to it.

My legislation tries to do this by making Mr. Anderson and Mr. Hartle victims so they don't have to actually suffer financial loss.

Mr. Anderson pointed out he never suffered any direct financial loss, but something has to be done, and I am trying to figure out a way to do it. It is true that the conduct of the Social Security Administration, in allowing his number to get out, and the conduct of those other agencies, the department stores in your testimony and, for that matter, the hospitals, we think of hospitals as different, but they are in there to make money just like everybody else. They perhaps could, I don't know, perhaps could have done a more thorough job of verifying the identity of that particular victim and not allowing you to be victimized.

Mr. ALBRIGHT. I would like to make one more comment.

I asked them specifically, Mr. Congressman, that question. How will we fix this problem? That is the obvious question to ask. While technology is not there today, as a consumer I hate to think about it, one thing that they kept coming back to me with is biometrics, fingerprints on credit cards, eyeball scans, and all types of things like that. And eventually in this society we may move, unfortunately, to that type of security to make sure that consumers are being protected.

Mr. SHADEGG. Yes. Retina scanners have been debated on the floor of the House in other contexts, welfare and otherwise, as perhaps one of the next steps that we need to go to.

And, you know, somebody in their testimony made the point that crimes of this nature—this is the crime today, but it will move forward just like less sophisticated crimes of 5, 10 years ago. And it

may be that, as a result of this law and as a result of other incentives imposed by Congress and, hopefully, rather than that as a result of your own initiative, we take steps which do not hamper commerce but in fact do stop people from doing to Mr. Anderson and my constituents what has happened to them.

I have used more than my 5 minutes. I yield back the balance of my time I don't have.

Mr. SHIMKUS [presiding]. I am not going to ask additional questions. I am going to reiterate what my colleague from Arizona stated.

I have been a member for 3 years, and I think it is safe to say that the congressional majority would rather have the private sector solve these problems. You do not want us imposing new burdensome laws and regulations and regress through the courts, but we will do that if we don't see a change in some of these activities.

I see three things. I see approval, then immediately stopping the undue harassment after the problem has been identified, and then eventually the prosecution arena.

We have some Federal agencies that do a great job. The SEC works with the industry to police itself. They work very closely. I would just encourage those who are in the industry and with the help of the Federal Government to sit down rapidly and talk since you all are doing the work. You all know better than we do, and I would suggest working with obviously the No. 1 champion here on the House side, Mr. Shadegg, working with him to address this before we do it with the heavy hand of government, work with us to find a pro-business approach to solve these dilemmas, and I would be happy to help in any way that I can.

With that, I am going to adjourn this hearing. Thank you very much.

[Whereupon, at 12:25 p.m., the subcommittee was adjourned.]